

Re: [fw-wiz] IPS vs. Firewalls (why vs. ?)

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-02/msg00072.html>

- *From:* "Marcus J. Ranum" <mjr@xxxxxxxxxx>
 - *Date:* Fri, 03 Feb 2006 12:32:39 -0500
-

Gabriele Buratti wrote:

3) new technologies:

- reassemble the fragments in a separate space, do the checks, then if ok send the fragments (no session rewriting).
- focus on the "strange things won't be forwarded", rather than signatures: faster, sharp, you can use the marketing wizard's "0-day protection" word :)
- decode recursively to stop blended attacks
- don't use a proxy: check on the fly and if test is passed then forward the packet (so no session rewrites and no dangerous listening ports)

I seem to remember a discussion similar to this back in 1992... Of course then it was proxy-versus-stateful firewalls. :)

What you're doing is your confusing features with implementation and are talking about the performance results of implementation as if it has something to do with the value of the features. The original implementation of proxies, as separate processes atop an O/S kernel, was because it was convenient to implement and the O/S interprocess memory protection was a useful feature. If you extend that line of thinking a bit, making each process use socket-level abstractions leverages the O/S' IP stack effectively to do reassembly and error correction. Again, those are useful attributes of an O/S kernel and so we used them. But, if you think about it for a bit, there's little difference (other than implementation details) if you had a device that did full TCP state-tracking, packet sequencing, IP checksumming, etc -- most of the features of an IP stack -- in silicon in the packet-shuffling loop of a switch. As long as it's doing the right error checking and doing it correctly it's irrelevant from a security standpoint whether it's implemented as a separate process or in some state machine someplace else. What matters is, and always will be, the error checking and security processing that's done and how rigorous it happens to be. What shouldn't come as a surprise to anyone is that the amount of CPU power it takes to do IP processing in an IP stack is about comparable to the amount of CPU power it takes to do the same IP processing in a state engine in a

subroutine.

The way to get performance gains is, simply, to cut corners. Do you want your IP processing to get 1/3 faster? Don't check the checksums! There are a number of commercially significant firewalls from the old days that did exactly this and gained significant market-share by being demonstrably faster than their competitors. And, you know what? It worked fine because at that time the hackers didn't have readily accessible packet-crafting tools and DOS attacks weren't fashionable yet.

Now, we come to the meat of the matter – the security industry's customers have demonstrated that they are always willing to trade for the perception of performance over the perception of security.(*). Of course, nobody really understands what checks, internally, their product of choice makes. Indeed, most vendors don't, either. They simply hope it will be the right combination of checks to defuse the current and (hopefully!) the next attack.

So, what you're saying is that your product is doing a blend of checks and is doing them as fast as it can. That's great!!! The fundamental issue always boils down to whether your product inherently implements default permit or default deny; what it does with the stuff that it will, inevitably, encounter that is outside of its knowledgebase. My concern with IPS is not the implementation but the idea – the very premise of IPS is to permit everything but try to shoot down that which is discovered (on the fly, I may add) to be bad. Fundamentally, that's a stupid idea. So, perhaps you have a good implementation of a stupid idea; good for you. I've been saddened to see that nobody has done to the design table and tried to make a fast implementation of a good idea, instead.

mjr.

(* There are a few outliers – hi Dave!)

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxx
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>