

## RE: [fw-wiz] Application-level Attacks

**Source:** <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2005-02/0067.html>

---

**From:** Marcus J. Ranum ([mjr\\_at\\_ranum.com](mailto:mjr_at_ranum.com))

**Date:** 02/19/05

To: "Ofer Shezaf" <[Ofer.Shezaf@breach.com](mailto:Ofer.Shezaf@breach.com)>, <[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)>

Date: Sat, 19 Feb 2005 10:27:42 -0500

Ofer Shezaf wrote:

>Applying science to the issue is a real problem since organizations  
>don't publish such incidents.

That's a big part of it, and it has lethal side-effects. So here is how it happens:

- many organizations won't publish about incidents
- so, in response, security organizations try to find out using anonymous polls
- unfortunately, these polls are filled out by those who are
  - a) bored
  - b) just having fun
  - c) have an agenda(in statistics this is called a "self-selected sample" and they teach you in stats 101 that they never give valid or worthwhile results)
- since the polls are anonymous it's impossible to cross-check them for accuracy.

Case in point on the last item: last week I recieved 2 copies of the CSI/FBI poll. Email me if you want me to send you a scan of it. What's interesting is that a) I got 2 copies and b) it's anonymous. So do I fill one out for "ranum.com" and one for "tenablesecurity.com"? Or - what? Do I even care enough to fill one out at all? Or even both?

None of that is science. Science is about controlling inputs and repeatability.

>As a result there is a bias in the  
>security community mindset towards large scale attacks such as worms  
>that are difficult to hide and get all the publicity, but may actually  
>cause much less damage than a targeted attack.

I think you're right. It's what makes the industry increasingly hype-driven.

There's the old "80% of attacks come from the inside" which I still hear quoted (even though it is utterly wrong and it's a number

## Firewall–Wizards: RE: [fw–wiz] Application–level Attacks

someone pulled out of a cracker jack box back around 1989) but nobody knows. NOBODY KNOWS. So instead we are fed hype. Because nobody knows and there is no science here, Gartner analysts can get away with making ridiculous claims because you can't refute them.

By the way, the way to refute those claims is to ask about their methodology and don't stand for vague answers.

*>We hardly ever hear about a successful SQL injection attack in which  
>sensitive information was stolen or fraudulent transaction was  
>committed, but we here a lot about worms that mainly cause site down  
>time. On the other hand my personal experience as well as the experience  
>of others shows that in far too many penetration tests we find  
>vulnerabilities such as SQL injection.*

Right! And because everyone is hyped up about whatever the marketeers are hyping, all the time and \$\$ get spent on the wrong thing ("lets put in an IPS that costs \$60,000 instead of tightening our firewall rules down from "Stupid" to "Merely Dangerous") Because there's a flood of marketing chasing the hyped dollar, you have people doing complicated dumb stuff instead of cheap simple smart stuff. (usually "cheap simple smart" security consists of NOT DOING SOMETHING, which almost always costs less or next to nothing)

*>One interesting paper which tries to measure the internet security  
>status based on results of penetration tests is "How safe is it out  
>there?"  
>[http://www.imperva.com/application\\_defense\\_center/papers/how\\_safe\\_is\\_it.html](http://www.imperva.com/application_defense_center/papers/how_safe_is_it.html)*

I'd feel better if the paper were not from a vendor selling solutions to the problem they are identifying. That's good marketing, of course, and is perfectly legitimate, but it puts my Capt Kelly BS Detector's sensitivity knob on setting 11.

*>Most attempts I've seen to quantify the threat where based on user  
>surveys and where very far from technology.*

Yep, user surveys are bogus. I've read 'em all and been shocked by the stats–101–level methodological errors in them. Last time CIO magazine did a security survey I contacted the folks who wrote it and sent them a nasty mini–dissertation containing a summary of introductory–level testing methods. The response I got was characteristic:

"Why are you attacking our survey? Sure it has some methodological errors but it's the best we could do, and at least the numbers are interesting and they are better than nothing."

No, in fact, they are worse than nothing because they are

misleading...

Dan Farmer did an interesting survey in 1996 (<http://www.trouble.org/survey/>) where he tested a random sampling of hosts with SATAN. His methodology is actually pretty good, and shows signs of scientific thinking (he uses a control study and a randomly selected sample...) It'd be neat-o if he'd run it again and we could see if Intrusion Prevention has really solved the problem like all the marketing weenies said it would. ;)

mjr.

---

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