

# Re: [more specific] Signature vs. Protocol Analysis

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2002-03/0096.html>

---

**From:** Stephen P. Berry ([spb@meshuggeneh.net](mailto:spb@meshuggeneh.net))

**Date:** 03/12/02

To: "Marcus J. Ranum" <[mjr@nfr.com](mailto:mjr@nfr.com)>

Date: Mon, 11 Mar 2002 16:56:31 -0800

From: "Stephen P. Berry" <[spb@meshuggeneh.net](mailto:spb@meshuggeneh.net)>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Marcus J. Ranum writes:

>>It took folks deploying firewalls a long time to figure out that an  
>>implicit allow rule with a bunch of explicit denies tacked onto it  
>>isn't (typically) a sane way to develop a firewall ruleset.

>No it didn't!!!

Objection noted. I didn't mean to suggest that --nobody-- figured it out a priori. I was referring to the general case.

Security stupidity has three basic stages:

- 1) Everyone --should-- know better, but only a few hepcats actually do.
- 2) Everyone --is expected-- to know better, but a bunch of cretins still don't.
- 3) Everyone --gets sued-- for not knowing any better, more or less independent of whether they did or not.

I think firewalls are more or less in the second stage now, but IDS technologies are either at the first stage or are still in the unlisted zeroth stage (nobody knows about it at all except a mad scientist and an hunchback or two).

>>How long

>>is it going to be before we NIDS goons figure out the analagous truth?

>Some of us have been saying the analogous truth there all along, too,

>but again it'll take time and reality for it all to sink in. :)

Noted. I think there are a couple of problems adversely affecting reality's buoyancy in the matter:

Re: [more specific] Signature vs. Protocol Analysis

## SecurityFocus IDS: Re: [more specific] Signature vs. Protocol Analysis

- Systems to implement the kind of NIDS heuristics in question are very, very difficult to shrinkwrap and droolproof. I.e., the parts list includes a set of opposable thumbs and a large forebrain, and those aren't in everyone's inventory nor on their budget. This hurts the marketability of the product.
- Since the number of organisations that perceive a need for –some– NIDS is far greater than the number of savvy NIDS users, there are a lot of people using some random NIDS who have no perceived need for anything different or better.
- Even among ostensible quote experts unquote, there's no real consensus about this sort of thing, and...
- It is difficult even for most informed and motivated professionals to discuss/argue the subject (witness the endless nomenclature threads on the various mailing lists).

A meaningful exploration of any of these problems is really beyond the scope of an email message to a public mailing list, but I'd like to segue into a comment on the last point.

There are actually a number of groups/projects/efforts/whathaveyou devoted to standardising security nomenclature in a number of areas (from things like IEEE and NIST publishing standards to things like the CVE). While this is –good–, I think it's terribly insufficient, and gets perhaps more attention than it's worth. Agreeing on a standard nomenclature is an important basis for technical communication, but at base it's still very primitive stuff...Og the caveman pointing at things and naming them.

What would be very useful, I think, is a formal –grammar– of some sort for use in NIDS/IDS in general.

What got me thinking of this was reading technical papers. I was actually recently reviewing a number of papers on rule learning algorithms[0], and man oh man can those things get turgid. One of the problems is that an awful lot of their basic processes get described in paragraph after paragraph of text...because there aren't many closed–form notations for describing the kinds of operations used.

It seems like it would be a Big Win if we could notationally describe fundamental –processes– of intrusion detection (and information security in general[1]). As mentioned earlier, there are a number of projects that seem geared toward being able to describe in great detail individual packets and that sort of thing...but I think a simple, descriptive approach of this sort is inherently limited.

Does this make sense? Is there a perceived need or desire for that sort of thing among the comparatively erudite members of this list? Or am I just hallucinating a need where none exists?

– Steve

## SecurityFocus IDS: Re: [more specific] Signature vs. Protocol Analysis

-----  
0 Specifically thinking of applications in developing automated processes for describing baseline traffic for use in NIDSes.  
1 In cryptography, for example, one can already describe in great detail the function of a cryptosystem to anyone with a bit of number theory.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.0.3 (GNU/Linux)

Comment: For info see <http://www.gnupg.org>

iD8DBQE8jVI8G3kIaxeRZl8RAoFYAJ4t955zSf0vddZlUePJ/a+wbzS2mkgCeMK4J

IpHyXfZa5Jn3mmE/KXK/67c=

=hWiZ

-----END PGP SIGNATURE-----

---

- ***Previous message:*** [Baeder, Jason \(GEIO\): "Re: Use of Taps for IDS"](#)
- ***Maybe in reply to:*** [Martin Roesch: "Re: \[more specific\] Signature vs. Protocol Analysis"](#)
- ***Messages sorted by:*** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)