Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Using the right words

In reading the published refereed journal and conference literature in psychology, and in observing the educational process in psychology, I have been highly impressed by the systematic use of specific and reasonably well-defined language in the presentation of information. It seems that the social science of psychology has found that precise word usage in accordance with defined concepts is fundamental to effective communication, and that papers that fail to meet these standards do not survive the peer review process.

In information protection and digital forensics, the fields that I spend most of my time in, I have found almost the exact opposite to be true. While my professors in graduate school, where I studied information science (M.S.) and then electrical engineering (Ph.D.), insisted that I use specific language from the existing literature, and I eventually learned the lesson of trying to be precise and careful in my word usage, it seems that the fields I work in have failed to learn these lessons and apply them as well as has been done in the other fields I have been exposed to.

Maybe it's just good marketing?

One of the main reasons I have attributed to the lack of using historically defined terminology stems from artificial intelligence (AI), a field in which term after term was used in year after year to breathe new life into the funding base. While I can barely remember the right words for the machine that examines a series of conditions, acting on the first one that is true, and then loops through those conditions again (I believe it was originally called a "", "production system"), it was subsequently renamed to "expert system", "rule-based systems", "event-condition-action mechanism", and so forth. And there was probably another name before ... and after...

In the computer security field, we see renaming all the time, and new names for slight variations on old concepts. For example, phishing, pharming, vishing, wishing, twishing, and you name it -ishing, all forms of deception in which the communications media is used to create the illusion of a trusted source requiring confidential information, and which results in the taking of that information and its subsequent use for the perpetrator's benefit (and usually the victim's harm).

Locally defined terms

Of course I am not rallying against the definition of new terms. After all, I first used the term "computer virus" in a scientific paper, and followed it up with formal definitions, proofs, and a series of papers and other works on the subject. I also first defined the term "information assurance", which has come into widespread use, and a range of other terms that appear in the scientific literature. But on the other hand, in doing so, I use existing terminology where it existed, and don't define terms to market something old as if it were new.

There is also a place for defining terms in any given work, particularly for use within that work

or that context. For example, in writing papers, reports, or briefings, I commonly define terms for the purposes of the work and use them later on. If done properly, this can bring clarity to the work. For example, rather than repeatedly use a sentence or paragraph to refer to the same concept, I commonly define a word that can be understood in context, and where feasible, I use a term that conveys the essential meaning. Rather than call that concept a gno or some such thing, I might call it a "locally defined term", which I will do for the remainder of this short piece.

Terms of art

In the area of computer security, locally defined terms often become more globally used, to the extent that they meaningfully convey a concept of utility. For example, the locally defined term "potentially serious negative consequences" is one that I commonly use as a "term of art", sometimes putting it after "event sequences", another commonly used locally defined term that became somewhat of a term of art. Another such term is "risk aggregation", which is a concept that has been around for a long time, and thus has gone beyond the realm of a locally defined term to become more of a term of art.

In the digital forensics space, I have used locally defined terms like "email-like sequence" and "actual email", to identify particular circumstances in particular cases. These will almost certainly not become terms of art, because they don't convey a very universal concept. On the other hand, in a recent paper, I used a locally defined term "GCF-similar group", which I think has a good chance of becoming a term of art, because it defines something of fairly universal utility, and because I think that others will use it in speaking of the same issue in future papers. We all hope to create a term of art now and then, particular those of us who do research and write papers. Another one I recently applied is "information physics", the physics of digital systems. I am hoping that this one catches on in the digital forensics community because the underlying concepts are fundamental to the progress of the field - at least I think they are...

A call for community action - or not...

So here's the thing. I think that when people write papers, they should be careful to apply terms that already exist wherever possible. For example, the term "trace" is clearly a concept in forensics that should be applied to digital forensics, and the term "coverage" is clearly a term from engineering mathematics that should be applied to computer security issues. I think that authors should be careful to know enough about their fields and closely related fields to use well-know terms when available, and not define terms for concepts that already have terms.

But it's not just authors. I think that reviewers, and many of my readers are reviewers, should comment on the use of existing concepts and help authors to use terms of art where they exist rather than allowing the authors to invent new terms of art for terms of art that already exist. Similarly, when a locally defined term is used, it should not be used in place of a term of art that already covers the concept. The term of art should be identified and referenced, and the reviewer should insist on it. We shouldn't reinvent the wheel, unless there is a good reason to - but if there is a good reason, we should use a proper term for it. Cog perhaps?

