Report on the discussion of "A Cursory Examination of Market Forces Driving the Common Criteria"

Kenneth G. Olthoff
olthoff@earthlink.net
kolthoff@radium.ncsc.mil

"In the beginning was the beard, and the beard was Marv [1], and the beard was with Marv, and the beard was good. And lo, the commandments came down from on high, and the commandments were Orange, and the Commandments were good. Can I get an A1?"
<silence from the audience>
"No, and that's the problem. For it's known that we cannot surf both GOTS and mammon, and mammon has the market share, and so it was decided to consort with the gates (and windows) of industry, which is how we got to where we are today[2]."

With this somewhat paraphrased sermonette, delivered in the style one might expect from a fire and brimstone evangelist, Kenneth Olthoff summed up in highly abridged form the history of the computer security marketplace. Having gotten the attendees' attention with his unconventional approach, he then kicked off a discussion of economic issues surrounding the market acceptance of the Common Criteria and its supporting structure of Protection Profiles, Security Targets, and Evaluations.

Mr. Olthoff did not discuss the intrinsic value of the Common Criteria, or any other similar attempt to develop a market for security. Instead, Mr. Olthoff set forth the need to analyze whether the economic model of the Common Criteria will influence the various parties to behave in the desired fashion. Mr. Olthoff's analysis attempted to show that while the outcome was far from certain, a case could be made that the market might in fact lead users, vendors and evaluators to cluster on a few generic, and therefore less effective, Protection Profiles. Mr. Olthoff noted that this varied from the stated intent of creating a market for products that more closely addressed the needs of customer communities. Once the original position was laid out, the discussion opened up, involving most of the attendees.

1999 New Security Paradigm Workshop 9/99 Ontario, Canada

One of the first counter examples raised was the idea of small companies serving niche markets. The various vendors putting out industry-specific applications templates for databases and spreadsheets were offered as examples of instances where the market did not behave as predicted by Mr. Olthoff's analysis. Mr. Olthoff freely acknowledged that his analysis could be incorrect, and that the example was a very viable counter-argument.

Mr. Olthoff indicated that the main goal of his original submission was to get people to consider the economic influences on behavior. He attempted to clarify that the accuracy of his own analysis was of secondary importance, and that given his background and the limited amount of effort put into his analysis, it was assumed that a more skillful investigation of the issue was needed.

The discussion then headed in the direction of open source software, and whether the Common Criteria and similar schemes might provide a vehicle by which open source software might gain a foothold in the security community. While the attendees all seemed kindly disposed toward open source software, a brief discussion led to the conclusion that there were no inherent economic advantages or disadvantages that would lead open source software to fare differently from proprietary software in a marketplace governed by the Common Criteria.

Another topic that arose multiple times during the discussion was a comparison of the Common Criteria to ISO 9000. It was mentioned that in both cases, there is perceived value, but that the generation of paperwork required may add little value to the overall usefulness. It was pointed out that both ISO 9000 and the Common Criteria emphasize specific documentation in a rigorously specified format.

An additional note in the comparison was the difference between the ISO 9000 model and the Common Criteria. It was brought out that one part of becoming ISO 9000 certified is that a firm must have only ISO 9000 certified suppliers. Thus, the bigger firms become accomplices in spreading ISO 9000 to their suppliers,

[1] The reference is to Marvin Schaefer, one of the principal authors of the Trusted Computer System Evaluation Criteria, AKA "The Orange Book", and the possessor of a distinctive beard of the type made famous by the band ZZ Top. Mr. Schaefer was present, which was why he was singled out among the Orange Book authors. No disrespect to the other Orange Book authors or their beards (or lack thereof) is hereby expressed or implied.
[2] If memory serves, the actual wording included references to "making pacts with Beelzebill" and "the gates (and windows) of hell" – ED.

who spread it to their suppliers, etc. The attendees agreed that it would be difficult to spread the demand for the Common Criteria by similar means, given that there is not a hierarchical relationship between CC vendors, users and integrators. It was also noted that while ISO 9000 has been successful in the marketplace, other government instigated mandates such as GOSIP and "C2 by '92" were unsuccessful.

Another question discussed where the true benefits of the Common Criteria might lie. One opinion was that the value and success of the Orange Book was unrelated to, and unaffected by, the underlying economic model, but was instead based on capturing and conveying the state of the art at the time to a wider audience. This brought a response expressing concern about the quality of profiles and evaluations under the Common Criteria, since the Protection Profiles and Security Targets against which evaluations will be done may not be vetted adequately for security value and appropriateness. By contrast, the formulations of the various ratings in the Orange Book went through rigorous peer scrutiny for many years. It was also pointed out that the Common Criteria scheme allows one to separate assurance inherent in the design and development process from the strength of the mechanisms, while those two factors were coupled in the Orange Book.

Getting back to the non-technical drivers, a question was raised as to what factors might drive the acceptance of security products in the marketplace, whether under the Common Criteria scheme, or otherwise. The answers offered included legal liability, insurance requirements for security to gain favorable rates on insurance against loss, guarantees, auditors, and actuaries. One interesting observation was along the lines of "After all the Y2K lawsuits are over, those computer-literate lawyers will be looking for places to put their knowledge to use." There seemed to be consensus among the attendees that some mechanism is needed to create and enforce liability and responsibility for the consequences of security failures. Whatever the mechanism might be, it should apply to those operating the systems, and those designing and selling them.

The general conclusion seemed to be that eventually, security would need to be mandated, either by private means, such as trade associations or the insurance pricing structure, or through government legislation. There seemed little confidence among attendees that security would be a pull function where users demanded it, but that it would instead be a push function, where other agents levied a requirement for security on the users. There were some comments implying that such a push would only work when the awareness among users was sufficient to not actively oppose the imposition of security.

While there seemed to be sufficient interest and opinion to continue discussion of both the specifics of the Common Criteria scheme, and the general concepts of economic forces influencing the security marketplace, the time limitation on the session brought the discussion to a close.