The Cybersecurity Threat Lurking in End-User License Agreements

Position Statement in Response to *White House Executive Order* of May 12, 2021

Barton P. Miller
Vilas Distinguished Achievement Professor
Sohi Professor in Computer Sciences
University of Wisconsin-Madison
bart@cs.wisc.edu

Elisa R. Heymann
Senior Scientist
University of Wisconsin-Madison
elisa@cs.wisc.edu

This position statement addresses the area of the Secure Software Development Lifecycle. In particular, we address a critical issue that severely hampers the software community's ability to evaluate security tools, including those for static and dynamic analysis.

The basic issue is the restrictive nature of the End User License Agreements (EULAs) that come with commercially produced analysis tools. These tools typically come with licenses that prevent the user of a tool from reporting or sharing any of the results that they get from running the tool.

Such restrictions are more than a commerce issue; they severely impact our ability to evaluate the effectiveness of the tools that we are using to secure our national infrastructure. While these tools can produce useful results, they are not mathematically sound, so can provide no guarantees as to what they will report and not report. As a result, it is critical that independent third parties – such as government organizations, academic research groups, and consumer protection groups – be able to study and evaluate the effectiveness of these tools, independent of the efforts and interests of the tool vendors. Most users of such tools are not prepared or qualified to do such a comparison themselves, so are dependent on what they are told by the company that produced the tool.

It is not in our national (and global) interest to have this significant blind spot. This Executive Order explicitly specifies the use of such tools in paragraph 4(r), however users of such tools must blindly accept the producers' assurances of the effectiveness of such tools. In almost every other field except software, we allow the unbiased and independent evaluation of products. We have NIST setting standards; we have organizations like Underwriters Laboratories evaluating products; we publications like Consumer Reports producing product evaluations and comparisons; and we have academic groups providing in depth studies of effectiveness. This type of restrictive EULA (sometimes called "Dewitt Clause) dates back to 1983 when Oracle modified their license agreement in response to a conference paper that compared the performance of seven database systems (including Oracle's).

The EULAs being used today for security analysis tools shutdown any public discussion and community awareness related to effectiveness of the commercial tools.

We can see this effect in some examples from EULAs of currently produced commercial static analysis tools:

Example 1:

> **2.0 GRANT OF LICENSE AND USE OF SOFTWARE**
>
> …

2.2 **Usage Rights**. ... You shall not ... (e) perform, publish, or release to any third parties any benchmarks or other comparisons regarding the Software or User Documentation.

Example 2:

2 Limitations on Software Use. You may not:

…

2.2 disclose Software output, including by not limited to the results of any benchmark test of the Software, or Software documentation to any third party without XXX's prior written approval;

Example 3:

2. 2 **Conditions**. The rights granted to Customer above are conditional upon Customer's compliance with the following obligations:

...

Customer will not disclose to any third party any comparison of the results of operation of XXX' Licensed Products with other products.

To illustrate the need for such studies, we can look at a paper that we published in 2009[1]. Given the license agreements of the day from two of the most highly-regarded static analysis tools, Fortify and Coverity, we were able to publish results of these tools, as compared to the results from a detailed manual analysis performed by a skilled security analysis. This study showed that the tools were able to find only a small percentage of the serious security vulnerabilities found by the analyst (high false positive rate). In addition, the tools reported thousands of weaknesses (flaws) in the code that did not turn out to have security implications (false positives). And the capabilities of the two tools clearly differed. Of course, both tools now have licenses that prohibit any further publications of such results. Interestingly, years later, the legal group from one of these companies demanded that our university rescind this 2009 paper. Fortunately, our university lawyers fought this encroachment and prevailed.

Without regulatory or legislative action in this area, we are dependent on statements of the marketing groups in these companies.

[1] James A. Kupsch and Barton P. Miller, "Manual vs. Automated Vulnerability Assessment: A Case Study", *First International Workshop on Managing Insider Security Threats (MIST 2009),* West Lafayette, IN, June 2009. `http://pages.cs.wisc.edu/~kupsch/va/ManVsAutoVulnAssessment.pdf`