Software Diversity: Security, Entropy and Game Theory

Saran Neti and Anil Somayaji, *Carleton University;* Michael E. Locasto, *University of Calgary*

The committee felt that the simplifying assumptions in the modeling were a reasonable starting point, but that the authors oversold them as reflecting reality. For example, it is not reasonable to assume that all hosts have roughly the same number of vulnerabilities, clearly some systems are more hardened than others. Additionally, the paper spends a fair bit of space on how to measure diversity, but unfortunately, does not derive any unique insights from that approach. There was much interest in the proposed variant on capture the flag, both in general and as proposed method to provide useful information in measuring the proposed model. However, it does raise questions with the game theoretic analysis that was performed. Specifically, in game theory, with Nash Equilibrium the assumption is that each player understands the strategies available to other players, and in the proposed modification of capture the flag game this is simulated to some degree by broadcasting the information on which systems are using which software. However, in practice, it is often not the case that all agents can switch between all products due to software compatibility or policy reasons, and further due to competitive reasons it is often not clear which systems are using which software. In general, the committee was interested in the formal study of software diversity, and the attempt to provide a model with a proposed method for testing it. Everyone agreed that such a work would create interest and discussion.