Ryan Ponstein

Dr. Walter Schilling

SE-4930 –Secure Software Development

8 February 2012

Article Review #4: Demythifying Cybersecurity

A significant part of computer security education is tackling myths that support much of the practice in the field. The article, "Demythifying Cybersecurity", focuses on four myths that recur in both popular literature and technical work: more layers of defense are always better than fewer; running my executables on my data on my system is secure because I control my system; effective security is necessarily burdensome; and trusted computing eliminates the need to trust people. The article was written by Edward Talbot, of Sandia National Laboratories, Deborah Frincke, of Pacific Northwest National Laboratory, and Matt Bishop, professor at the University of California, in the May/June 2010 issue of IEEE Security and Privacy.

The first myth discussed was that more layers of defense are always better than fewer. These layers protect the "crown jewels" by strictly enforced logical and physical layers of security mechanisms. While history has shown that the layered defense is well suited for protecting physical assets, the authors argue that the layered defense has proven less and less adequate when applied to information systems' exponentially growing scale and complexity. A layered defense can limit the ability to protect cyber assets and the interaction between layers can reduce protection. The second myth discussed was that "running my executables on my data on my system is secure because I control my system." The authors assert that this myth is based off the assumption that you can truly control your system and that you understand precisely what security policy is implemented by the controls you select. In addition, a system's complexity

and changes in the threats that can affect that system make control a myth. The authors use the example of an expanding company and Microsoft's development of Windows Vista to prove their assertions. Their solution is to that education can focus on the difficulty of assessing the actual result of combining security mechanisms. A penetration study could illustrate that even though you may control your system, aspects of the environment might weaken system security even if your control is perfect. The third myth is that effective security is necessarily burdensome. The myth holds that a system with visible, elaborately applied security measures is more secure than a system without this elaborate protection. The authors combat the myth by stating that security mechanisms should be looked and implemented in regard to usefulness and effectiveness, not just to be burdensome. They look at three-factor authentication and whether it really prevents more hackers from accessing the system than with a two-factor or one-factor authentication. They emphasize that each added security mechanism should be justified by ample research in combating an issue. The fourth myth is that trusted computing eliminates the need to trust people – "if only we had no users, the system would be secure." The authors state that while usually the focus is on points where the system trusts external information or fails to validate data, the "people" points should not be overlooked. A computer simply follows instructions and designers, creators, and users must be investigated. If one these people is not trustworthy, neither is the computer.

Overall, the authors believe that we can move from myth and folklore to formalizing our approaches by making hypotheses and experimentally validating them. Myths can be replaced by critical thinking and science. Through reading this article, I learned that these myths can be quantified and examined critically. Secure software development can be improved as we move away from just implementing security mechanisms due to myths, not established justification.