

Software Security

Jeannette M. Wing
Computer Science Department
Carnegie Mellon University
Pittsburgh, PA 15213 USA
wing@cs.cmu.edu

Abstract

Security vulnerabilities are increasingly due to software. While we focus much of our attention today on code-level vulnerabilities, such as buffer overflows, we should be paying more attention to design-level vulnerabilities. Independently designed and implemented components may individually behave properly, but when put together, unanticipated interactions may occur. An unanticipated interaction between two software components is an opportunity for an attacker to exploit.

In this talk I will discuss two research topics related to software security: security metrics and security policy composition. For security metrics, I will present a method for measuring a system's attack surface [1, 2, 3], which does not count vulnerabilities, but rather the ways in which an attacker can potentially enter a system and do damage. For security composition, I will present an algebra for describing composing security policies [4]. For both topics, I will present examples drawn from real software systems.

References

- [1] M. Howard, J. Pincus, and J.M. Wing, "Measuring Relative Attack Surfaces," *Proceedings of Workshop on Advanced Developments in Software and Systems Security*, Taipei, December 2003. Also CMU-CS-03-169 Technical Report, August 2003.
- [2] P.K. Manadhata, J.M. Wing, M.A. Flynn, and M.A. McQueen, "Measuring the Attack Surfaces of Two FTP Daemons," *Quality of Protection Workshop*, Alexandria, VA, October 30, 2006.
- [3] P. Manadhata and J.M. Wing, "An Attack Surface Metric," CMU-CS-05-155, Technical Report, July 2005.
- [4] J. Pincus and J.M. Wing, "Towards an Algebra for Security Policies," *Proceedings of 26th International Conference on Applications and Theory of Petri Nets*, Miami, FL, June 2005, pp. 17-25. Extended abstract.
- [5] J.M. Wing, "Beyond the Horizon: A Call to Arms," *IEEE Security and Privacy*, November/December 2003, pp. 62-67.