Hardening the Network from the Friend Within

L. Jean Camp

School of Informatics, Indiana University
ljcamp@indiana.edu

Abstract. The insider threat in the networked world is distinct from the insider threat in the traditional physical business realm in that the most dangerous networked insider may be the least intentionally malicious. This inadvertent enemy within enables access by malicious outsiders through technologically nave or risk-seeking behavior. These behaviors include consistent choices (e.g., permission configurations, monotonically increasing access control rights) and specific behaviors (e.g., opening email attachments, clicking on video links). The risks of these actions are invisible to the individual, and the risks are borne at least in part by the organization. Any change in this insider behavior must include incentives for risk-avoidance, risk communication, and enable risk-mitigating choices. By developing incentive mechanisms and interactions that communicate these incentives, the risk behavior of the authorized insider can be aligned with the risk posture of the organization. We have combined game theory for incentive design, risk parameterization for pricing, and risk communication to create risk-based access control. The presentation will include the game formulation, presentation of the mechanism for pricing behaviors, and the remarkable results of initial human subjects experimentation.

C. Boyd and J. González Nieto (Eds.): ACISP 2009, LNCS 5594, p. 249, 2009.