Prevention vs. Cure

Stephan Neuhaus

Universität des Saarlandes

Current methods used to prevent security policy failures (formal methods, verification, static program analysis and so on) all use deduction to arrive at their goal. We argue that deduction is unsuitable for the *analysis* of intrusions that have already happened. Instead, we promote inductive methods as a better alternative for the automatic analysis of break-ins. These methods use experiments that are automatically designed, carried out, and evaluated. We corroborate this claim with a prototype implementation [NZ06].

Literatur

[NZ06] Neuhaus, Stephan ; Zeller, Andreas: Isolating Intrusions by Automatic Experiments. In: *Proceedings of the 13th Annual Network and Distributed System Security Symposium*. Reston, VA, USA : Internet Society, Februar 2006. – ISBN 1–891562–22–3, S. 71–80