Formal methods and system security *

Damas P. Gruska

Institute of Informatics, Comenius University,
Mlynska dolina, 842 48 Bratislava, Slovakia,
gruska@fmph.uniba.sk.

Keywords: security, observations,, information flow, supervisory control, insertion function

Abstract

Formal methods enable us to formulate and hence formally check the systems security from various points of view. A large class of security properties is based on an absence of information flow between public and private or classified states, actions, or any other parameters. It is expected that an attacker has some knowledge about system design and can partially observe its behavior. Basically, we distinguish language-based and state-based security properties, referring to sequences of systems actions or states, respectively. If the system is proved to be insecure; we have several options on what to do next. We can redesign the system. We can express the quantity of information that could leak. We can employ a supervisor controller which prohibits some system's behavior that could reveal classified information, or we can use insertion functions, which by inserting some systems action can prevent leak of classified information. Unfortunately, the most of related properties like security itself, the existence of the supervisor controller, or insertion function are undecidable in general if the underlying computational model has Turing power. Fortunately, for finite-state systems and reasonable limited attackers power, they become decidable. On the other side, in many cases due to state explosion, complexity remains exponential.

* this work was supported by the Slovak Research and Development Agency under the Contract no. APVV-19-0220 (ORBIS).