World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:11, 2015

Opacity Synthesis with Orwellian Observers

Authors : Moez Yeddes

Abstract : The property of opacity is widely used in the formal verification of security in computer systems and protocols. Opacity is a general language-theoretic scheme of many security properties of systems. Opacity is parametrized with framework in which several security properties of a system can be expressed. A secret behaviour of a system is opaque if a passive attacker can never deduce its occurrence from the system observation. Instead of considering the case of static observability where the set of observable events is fixed off-line or dynamic observability where the set of observable events changes over time depending on the history of the trace, we introduce Orwellian partial observability where unobservable events are not revealed provided that downgrading events never occurs in the future of the trace. Orwellian partial observability is needed to model intransitive information flow. This Orwellian observability is knwon as ipurge function. We show in previous work how to verify opacity for regular secret is opaque for a regular language L w.r.t. an Orwellian projection is PSPACE-complete while it has been proved undecidable even for a regular language L w.r.t. a general Orwellian observation function. In this paper, we address two problems of opacification of a regular secret ϕ for a regular language L w.r.t. an Orwellian projection: Given L and a secret $\phi \in L$, the first problem consist to compute some minimal regular super-language M of L, if it exists, such that ϕ is opaque for M and the second consists to compute the supremal sub-language M′ of L such that ϕ is opaque for M′. We derive both language-theoretic characterizations and algorithms to solve these two dual problems.

Keywords : security policies, opacity, formal verification, orwellian observation
Conference Title : ICCSIT 2015 : International Conference on Computer Science and Information Technology
Conference Location : London, United Kingdom
Conference Dates : November 27-28, 2015