Model Based Analysis of Insider Threats - DTU Orbit (06/10/2019)

**Model Based Analysis of Insider Threats**

In order to detect malicious insider attacks it is important to model and analyse infrastructures and policies of organisations and the insiders acting within them. We extend formal approaches that allow modelling such scenarios by quantitative aspects to enable a precise analysis of security designs. Our framework enables evaluating the risks of an insider attack to happen quantitatively. The framework first identifies an insider's intention to perform an inside attack, using Bayesian networks, and in a second phase computes the probability of success for an inside attack by this actor, using probabilistic model checking. We provide prototype tool support using Matlab for Bayesian networks and PRISM for the analysis of Markov decision processes, and validate the framework with case studies.

**General information**
Publication status: Published
Organisations: Department of Applied Mathematics and Computer Science, Formal Methods, University of London, Middlesex University, Technical University of Denmark
Contributors: Chen, T., Han, T., Kammueller, F., Nemli, I., Probst, C. W.
Number of pages: 3
Publication date: 2016

**Host publication information**
Title of host publication: Proceedings of the 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)
Publisher: IEEE
DOI: 10.1109/CyberSecPODS.2016.7502350
Source: PublicationPreSubmission
Source ID: 127204456
Research output: Chapter in Book/Report/Conference proceeding › Article in proceedings – Annual report year: 2016 › Research › peer-review