New multi-objective approach for dynamic risk-driven intrusion responses

Chaker KATAR, Ahmed BADREDDINE

Frontiers of Computer Science, DOI: 10.1007/s11704-019-8175-4

Problems and Ideas

- Problems of intrusion detection and response systems
  - Have never considered risk models as recommended by ISO 27002 and ISO 27005
  - Have several drawbacks in cost factor assessment as well as in countermeasure selection
- Ideas (Proposed Method)
  - A new risk-driven intrusion response mechanism. based on a new risk model that complies with the ISO 27005 and FIPS 65

Fig. Information security risk management according ISO 27005

Fig. Proposed risk-driven response framework

Mains Contributions

1. **The risk assessment part**: which involves the identification of several parameters, related to detected attacks, target assets, supported vulnerabilities, and deployed security controls. Moreover, it includes detailed steps to estimate different parameters and evaluate basic risks incurred by a target asset due to detected attacks.

2. **The risk treatment part** which focuses on selection of the optimal security control subset to thwart a detected attack. Therefore, it is formulated as a MOP. This aims to determine the optimal security strategy that minimizes both attack risks and response cost with regard to the tolerated risk level and the allocated security budget, respectively. The implementation of the risk mitigation uses the multi-objective influence diagram (MID) technique.

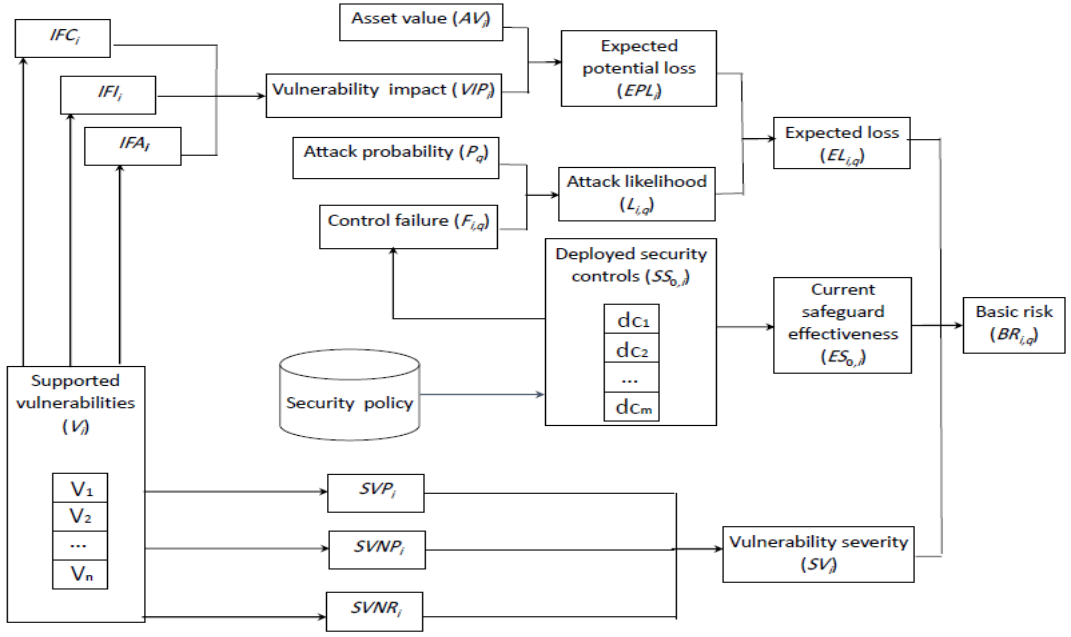

Fig. Risk model: graphical component (RM_G)

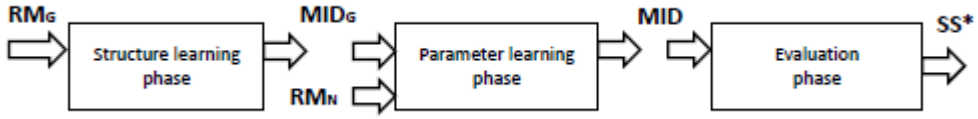

Fig. Risk treatment phases