A topology and risk-aware access control framework for cyber-physical space

Yan CAO, Zhiqiu HUANG, Yaoshen YU, Changbo KE, Zihao WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-019-8454-0
Problems & Ideas

• Problems: the interplay between the cyber world and physical world in the cyber-physical space proposes specific security requirements that are not captured by traditional access control frameworks.
  – The interplay between these two worlds proposes four types of security threats, including cyber threats, physical threats, cyber-enabled physical threats, and physical-enabled cyber threats. Hence, the physical security, the cyber security, and the interaction security should be all concerned in the access control model for the cyber-physical space.
  – The bad results caused by failure in providing secure policy enforcement may directly affect the controlled physical world.

• Ideas: we propose an effective access control framework for the cyber-physical space.
  – A unified access control model TAAC is proposed. It integrates the physical access control, the cyber access control, and the interaction access control.
  – A more rigorous policy enforcement method is needed to mitigate insider attacks.
Table 2 shows that the physical access control, cyber access control, and the interaction access control are unified in the TAAC model.

Figure 5 shows that for preventing insider attacks in the policy enforcement phase, the proposed method in this study is better than providing the role that minimizes the number of extra permissions.