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.

Main Contributions

Table 2: Role-permission assignment relation

Num	PA	Risk
p_1	$(visitor, enter, staffoffice, SL(visitor, mainarea) \wedge (SL(employee, staffoffice) \vee SL(manager, staffoffice)))$	20
p_2	$(visitor, enter, mainarea, SL(visitor, staffoffice))$	-10
p_3	$(visitor, login, cloudlet, SL(visitor, mainarea) \wedge AL(cloudlet, severroom))$	30
p_4	$(visitor, copy, file3, SL(visitor, mainarea) \wedge SA(visitor, cloudlet) \wedge AL(file3, cloudlet) \wedge AL(cloudlet, serverroom))$	20
p_5	$(visitor, delete, file3, SL(visitor, mainarea) \wedge AL(file3, visitor[phone]))$	-10
p_6	$(visitor, logout, cloudlet, SL(visitor, mainarea) \wedge AL(cloudlet, severroom) \wedge SA(visitor, cloudlet))$	-20
p_7	$(employee, enter, staffoffice, SL(employee, mainarea))$	10
p_8	$(employee, login, server, SL(employee, staffoffice) \wedge AL(server, serverroom))$	20
p_9	$(employee, copy, file1, SL(employee, staffoffice) \wedge AL(file1, server) \wedge AL(server, serverroom) \wedge SA(employee, server))$	20
p_{10}	$(employee, delete, file1, SL(employee, staffoffice) \wedge AL(file1, server) \wedge AL(server, serverroom))$	20
p_{11}	$(employee, logout, server, SL(employee, staffoffice) \wedge AL(server, serverroom))$	-10
p_{12}	$(employee, enter, mainarea, SL(employee, staffoffice))$	-10
p_{13}	$(manager, enter, saferoom, SL(manager, staffoffice))$	20
p_{14}	$(manager, open, safe, SL(manager, saferoom) \wedge AL(safe, saferoom))$	10
p_{15}	$(manager, enter, staffoffice, SL(manager, saferoom))$	-10

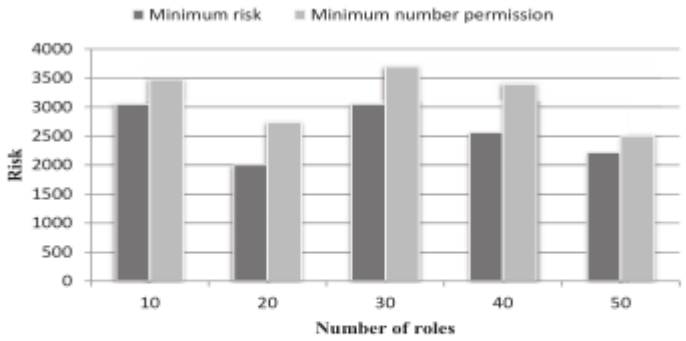

Fig. 5: Comparison of risk exposure for minimum risk method and minimum number permission method.

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.