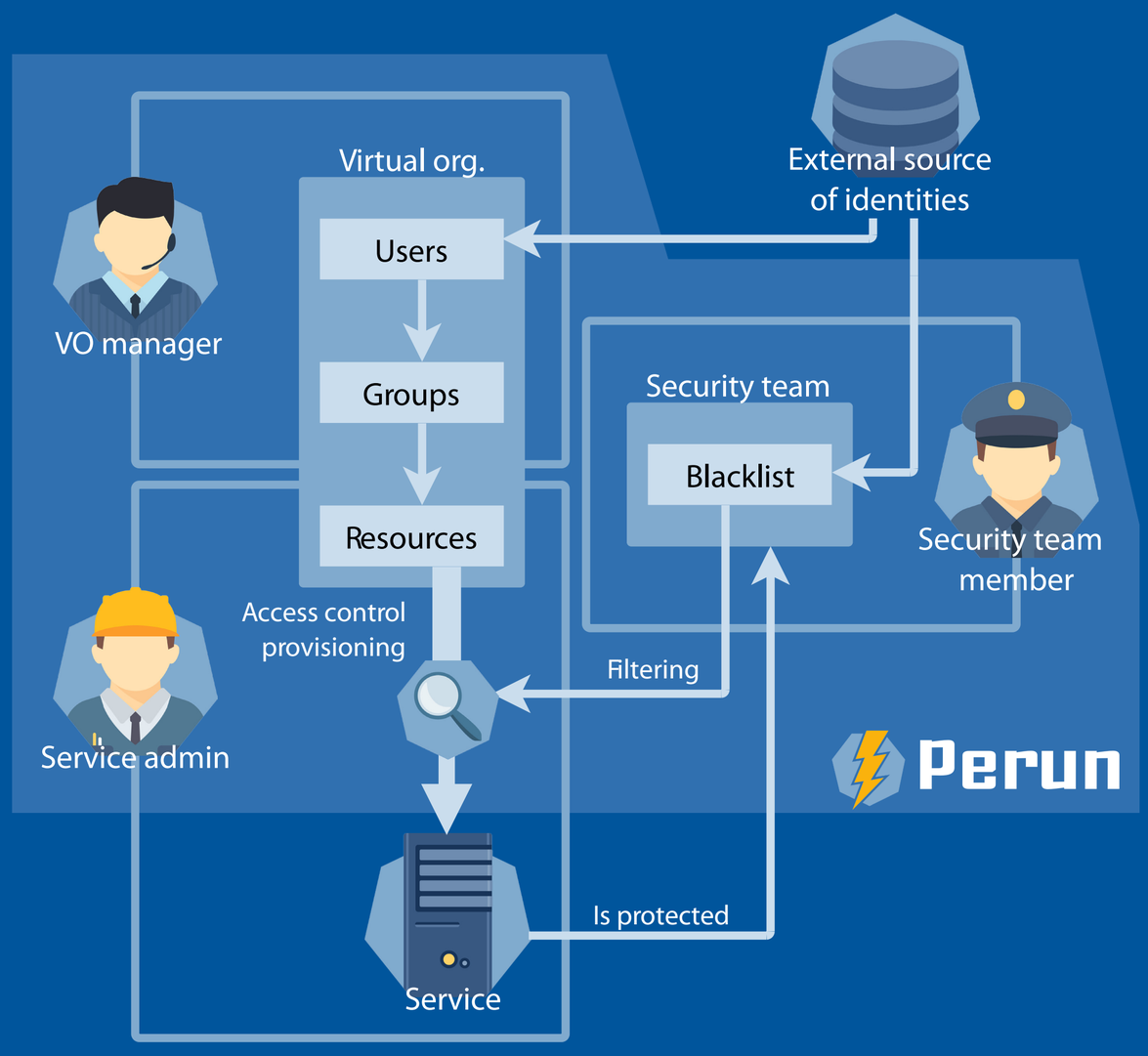
Incorporation of CSIRT Teams into Identity and Access Management Systems

Slávek Licehammer, Michal Procházka, Ondřej Velíšek – CESNET

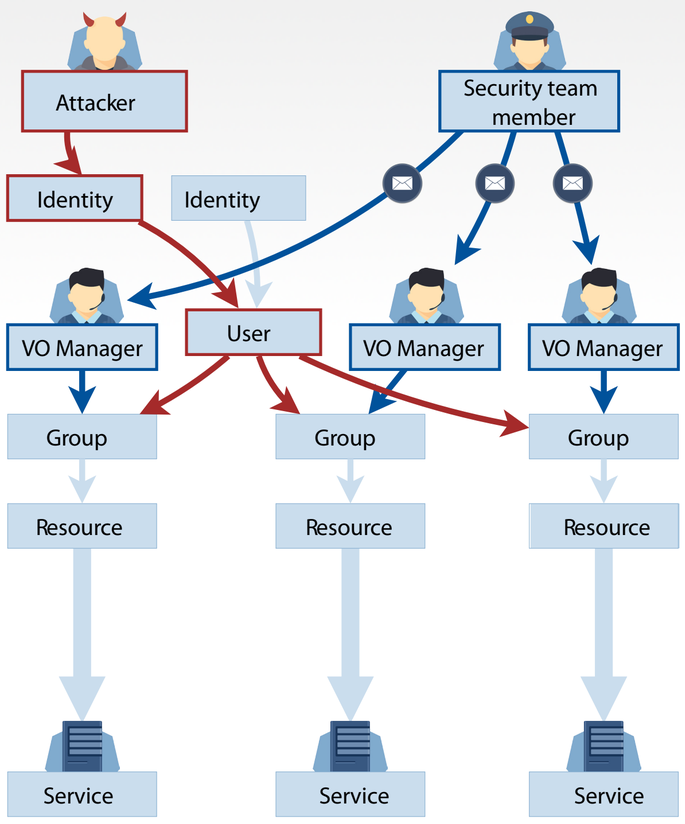
Using identity and access management system Perun, system administrator can delegate user management to VO or group managers. Moreover he can setup trust with CSIRT security team and by that **automatically suspend users** on managed service based on decisions made by the security team.

In case user account is compromised, member of CSIRT team can override access rights granted by VO manager which implies suspending access to user account **across all services** in the whole infrastructure. Perun can filter out banned users during access control provisioning process or use deprovisioning process to suspend active users on service level.



Security system integration benefits

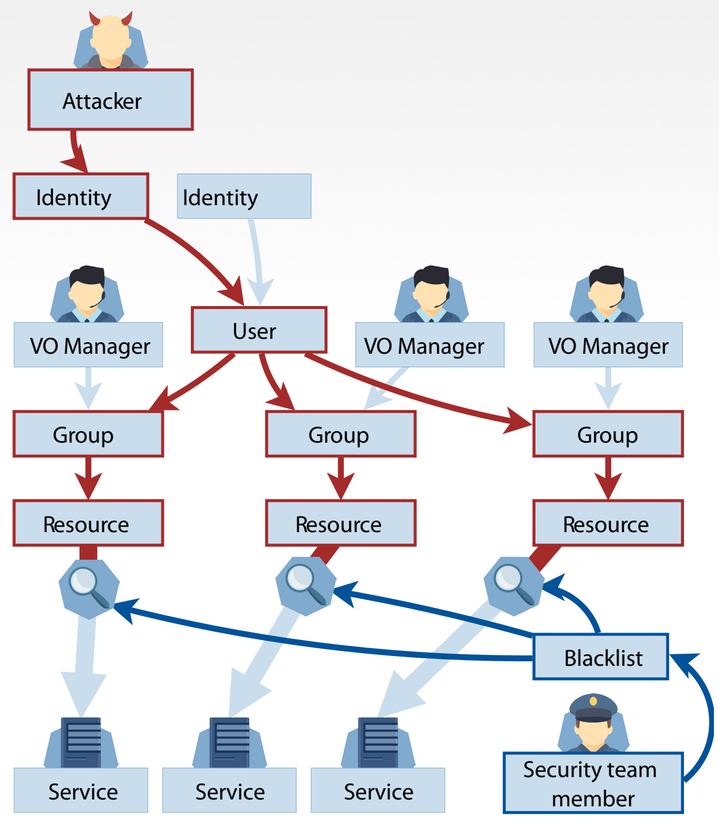
Current security system



Currently, CSIRT teams have to communicate with each VO manager to suspend compromised account. Typically, they use email communication which slows down overall security mitigation process.

Integration of CSIRT teams into identity and access management system enables **automatic immediate reaction** to a security incident. At the same time, the service administrator retains control of the whole process due to possibility of overriding or ignoring blacklist provided by security team.

Evolution of security system



Banning

Described architecture can be simply extended to support banning of users. Security team members can suspend the user or only ban him for a specified time interval. The rest of the architecture remains the same.

External authorization service

Members of security team do not have to interact with identity and access management system directly. Blacklisted identities could be imported from external systems such as ARGUS.

Developed by

Participating in

http://perun.cesnet.cz
perun@cesnet.cz