

Least Privilege, Segregation of Duties, and the Slow Rot of Privilege Creep

Sat, Aug 8, 10:00 AM EDT · <https://scottslab.io/posts/least-privilege-segregation-privilege-creep>



TL;DR

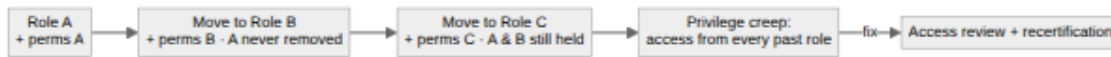
Least privilege gives people only the access their role needs; segregation of duties splits sensitive actions so no one person can complete them alone. Job rotation and mandatory vacation exist to surface fraud someone's been quietly covering. And privilege creep (the permissions people accumulate as they change roles) is the slow leak that undoes all of it, fixed only by regular access reviews with the managers who actually know who should have what.

Least privilege is the whole game in four words: the minimum access a role needs, and nothing extra "just in case." Spare permissions aren't convenience, they're standing risk. Every right an account holds is a right an attacker inherits the moment they land as that account.

Segregation of duties is least privilege applied to a single dangerous action: split it so it takes two people. Whoever requests a payment can't also approve it; whoever writes a change can't be its only approver. It isn't about distrust. Requiring collusion between two people is a far higher bar than requiring one person to be careless or compromised.

Two related controls are really fraud-detectors wearing an HR costume. Job rotation moves people through roles periodically, which spreads knowledge but mostly means a scheme someone's been

running gets inherited by a person with no reason to keep hiding it. Mandatory vacation is the sharper version: force someone out with no system access for a stretch, and anything they were manually holding together (a cooked reconciliation, a suppressed alert) surfaces while they can't cover for it. Fraud that needs daily babysitting doesn't survive two weeks of enforced absence.



The thing that quietly defeats all of the above is privilege creep. People change roles, the new permissions get added, and the old ones never get taken away. A five-year employee ends up holding a sediment of access from every job they've ever had, none of it reviewed, all of it live. You don't fix creep by hoping; you fix it with regular access reviews and recertification, sitting down with managers to validate each person's permissions against what they actually do now. Internal transfers are where it bites hardest, because revoking the old role's access is the step everyone forgets: adding the new access unblocks the person, removing the old access unblocks nobody, until it's the exact thing an attacker uses.