Authentication and Authorization in PHP

ROLE-BASED ACCESS CONTROL

Matthew Setter
PHP SECURITY ENGINEER

@settermjd matthewsetter.com

Module Overview

- Learn about Role-based Access Control
- What it is
- How it works
- Its advantages and disadvantages
- How to implement it in PHP

What is Role-based Access Control?

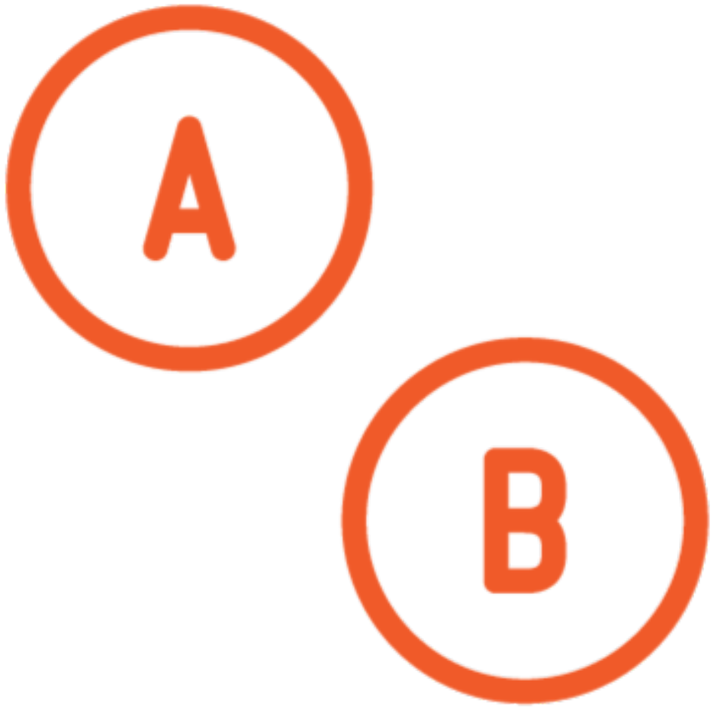
“Role-Based Access Control, or RBAC, provides web application security administrators with the ability to determine **who** can perform **what** actions, **when**, from **where**, in **what order**, and in some cases under **what relational circumstances**. In Role-Based Access Control, access decisions are based on an individual's roles and responsibilities within the organization or user base.”

Role-based Access Control - OWASP

“RBAC can be used to facilitate administration of security in large organizations with hundreds of users and thousands of permissions, *such as those in the Fortune 500 companies*.”

Role-based Access Control - Wikipedia

Differences to Access Control Lists

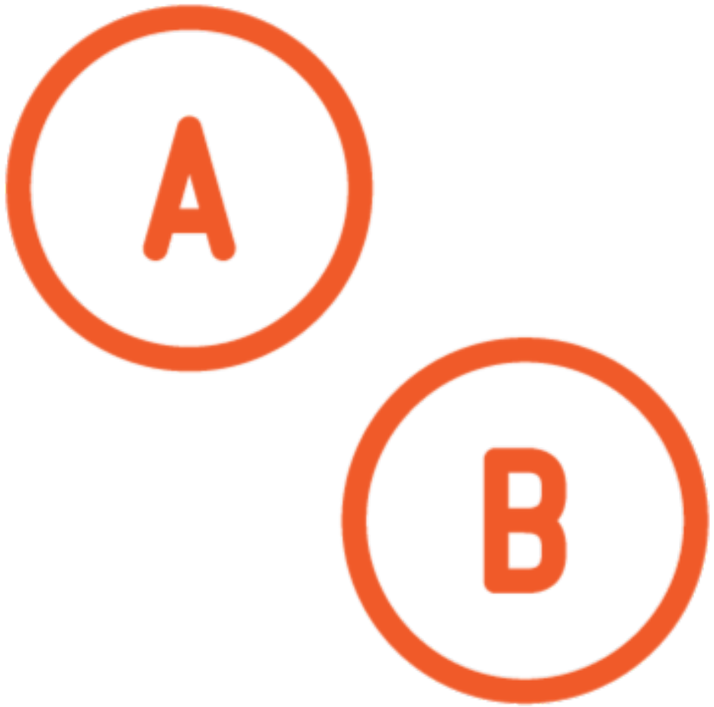


1. Works at the role level

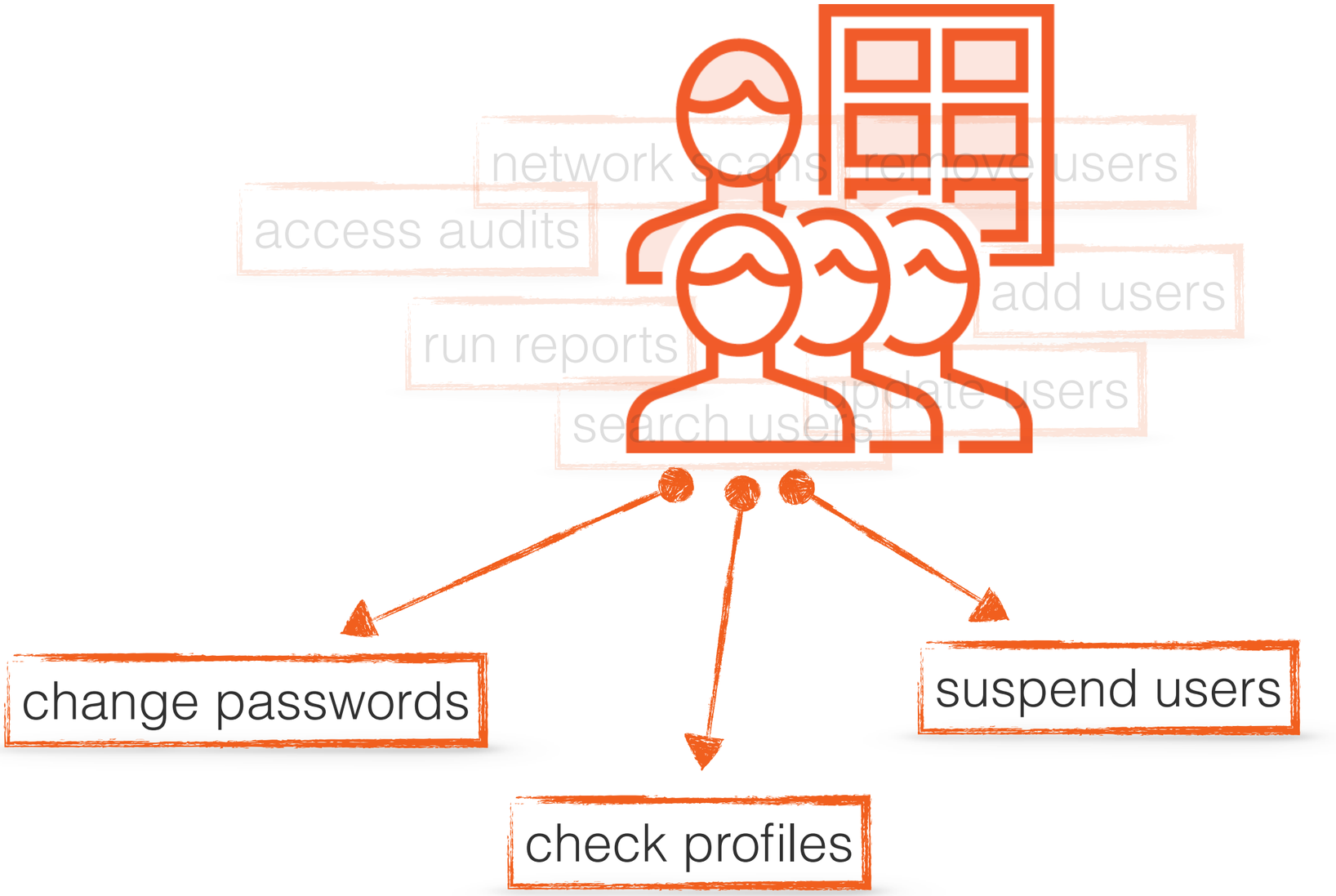
“An access control list could be used for granting or denying write access to a particular system file, but it would not dictate how that file could be changed. However, in an RBAC-based system, an operation might be to ‘create a credit account transaction in a financial application’ or to ‘populate a blood sugar level test’ record in a medical application.”

Wikipedia

Differences to Access Control Lists

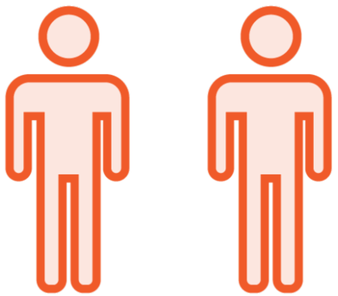


1. Works at the role level
2. Doesn't have the concept of a resource


network scans
remove users
access audits
add users
run reports
update users
search users
change passwords
suspend users
check profiles

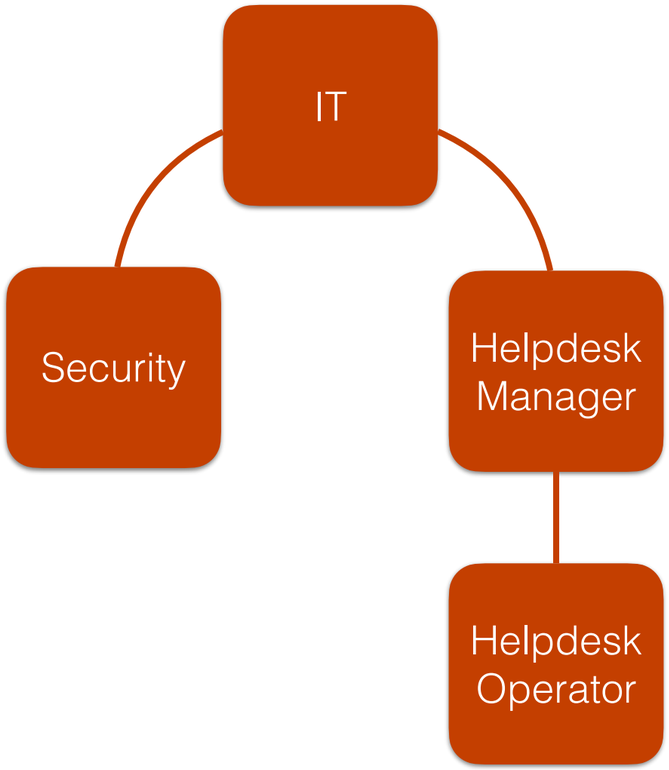
A Theoretical Model

Users

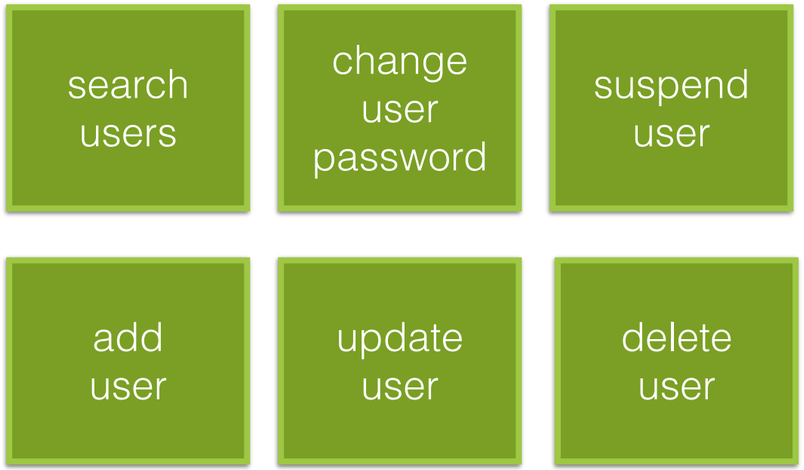


Jane Michael

Roles

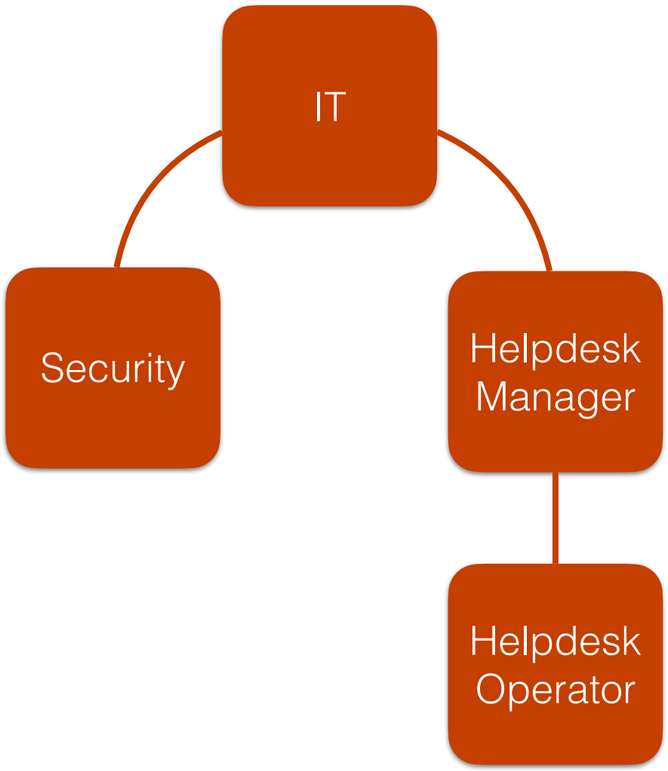


Permissions



A Theoretical Model

Jane Michael



search users

change user password

suspend user

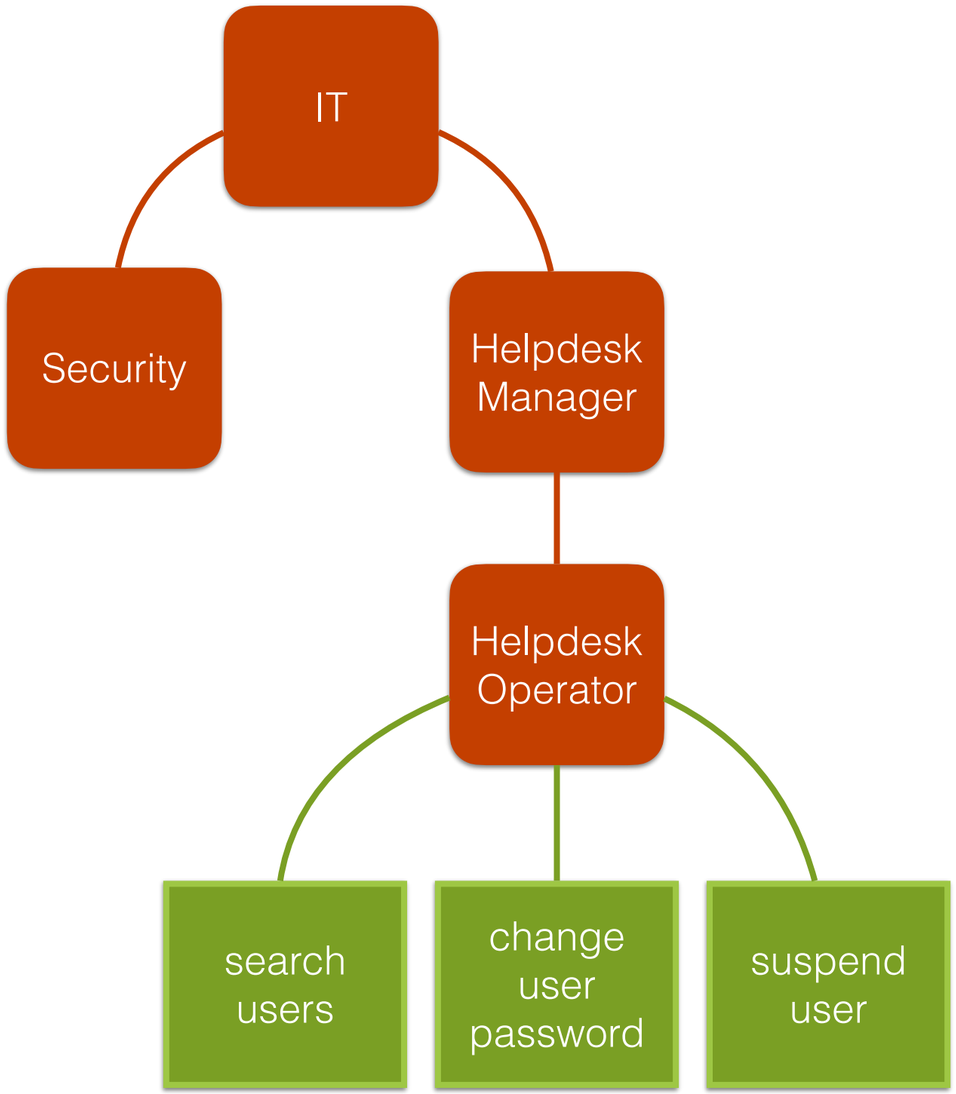
add user

update user

delete user

A Theoretical Model

Jane Michael



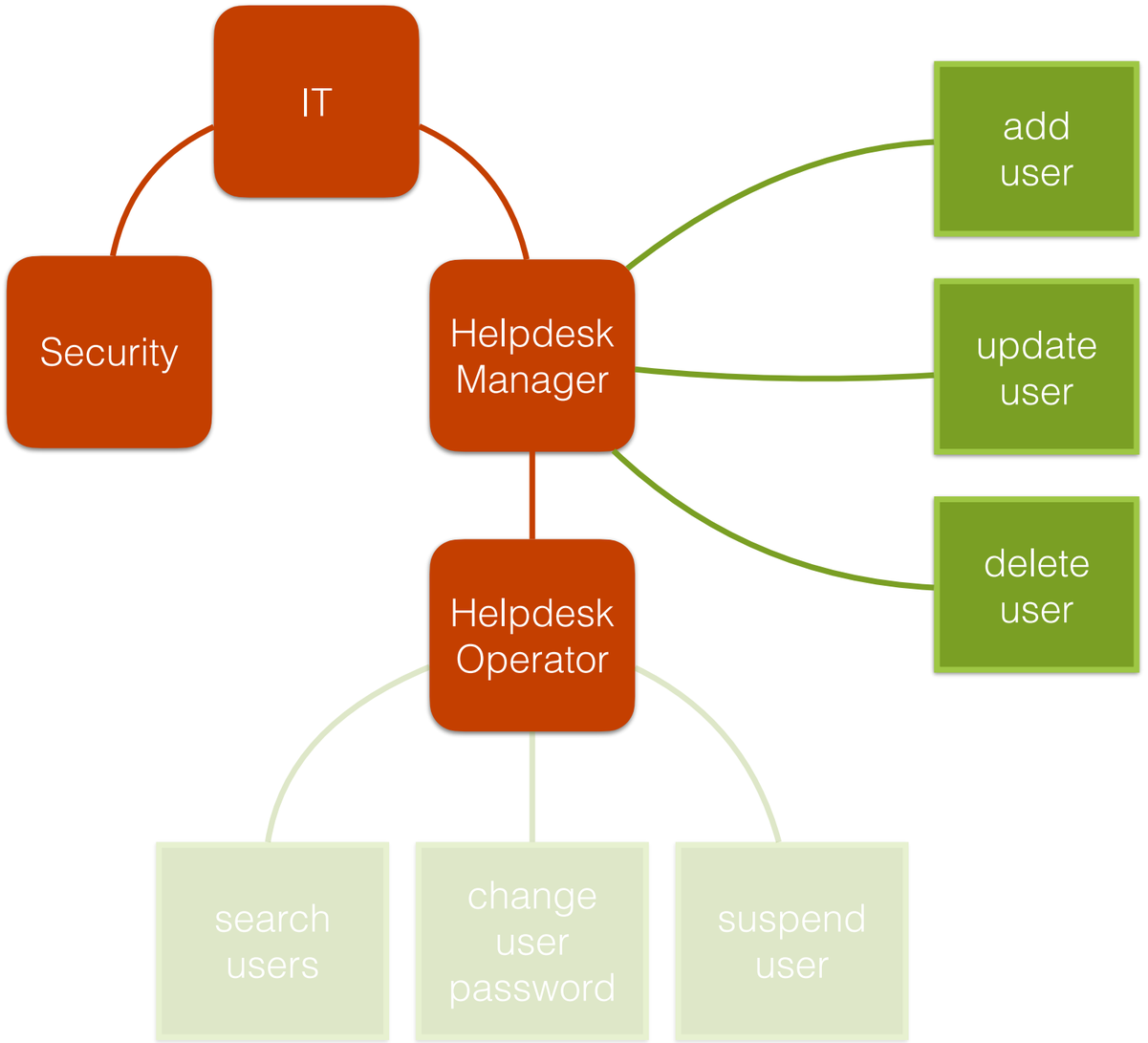
add user

update user

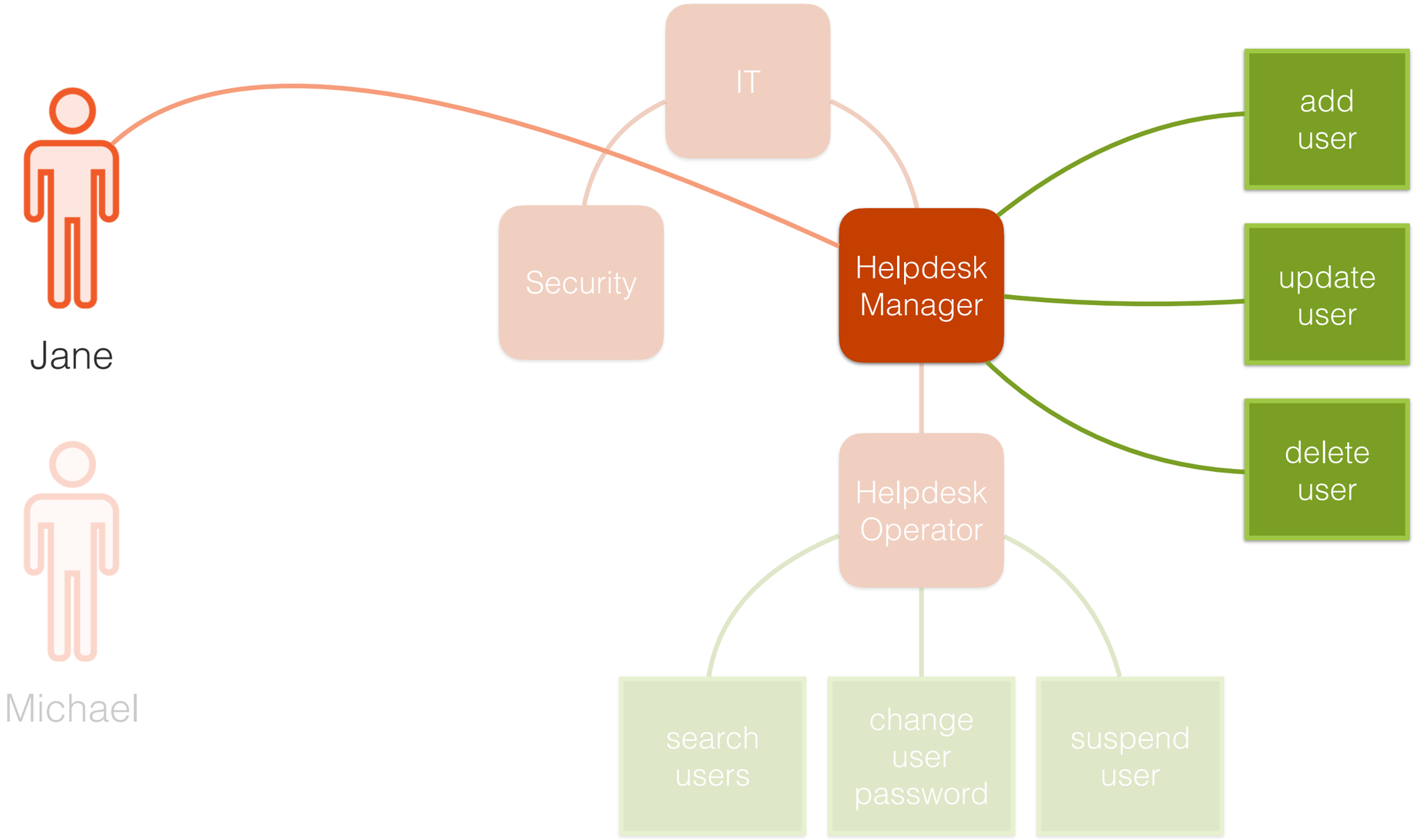
delete user

A Theoretical Model

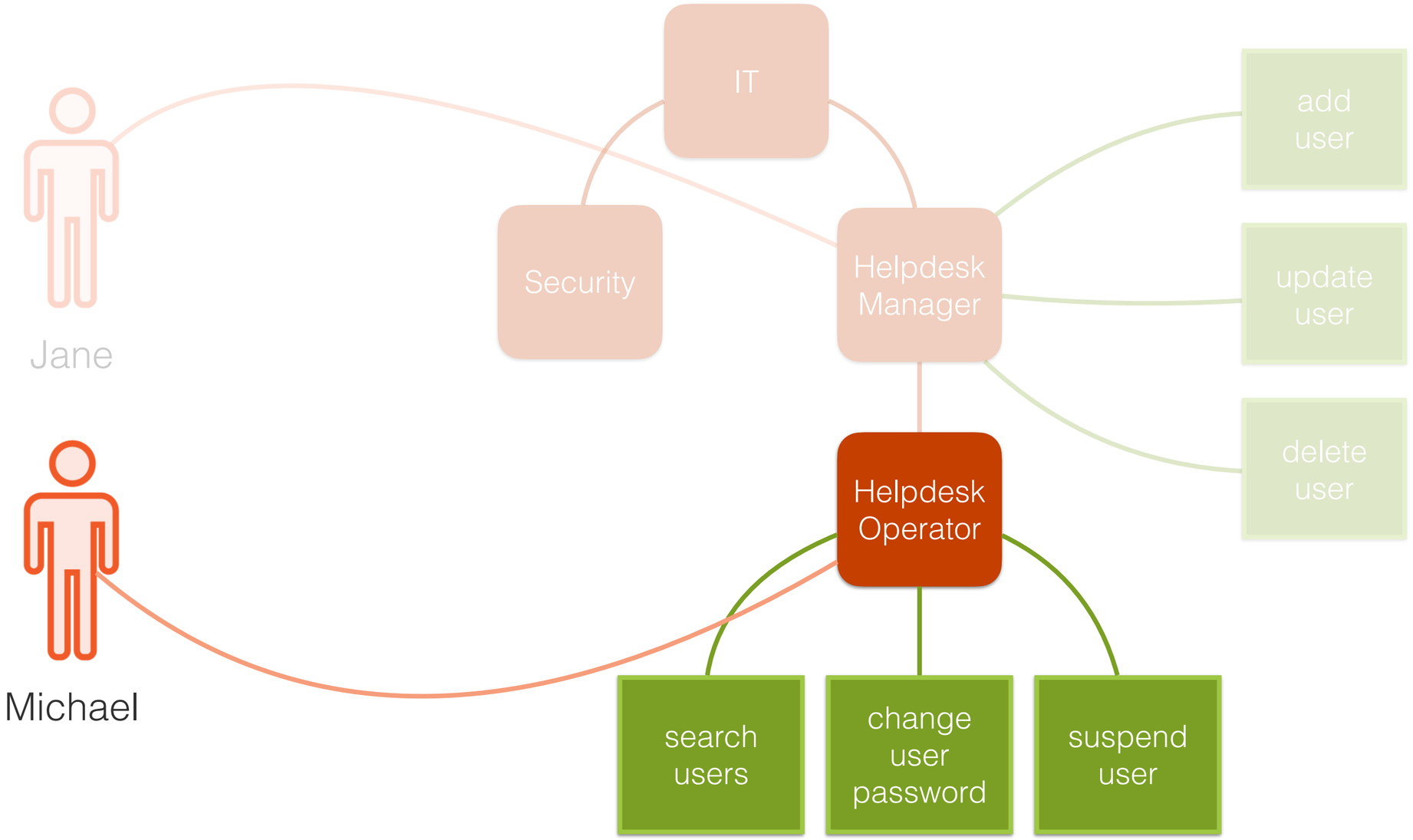
Jane Michael



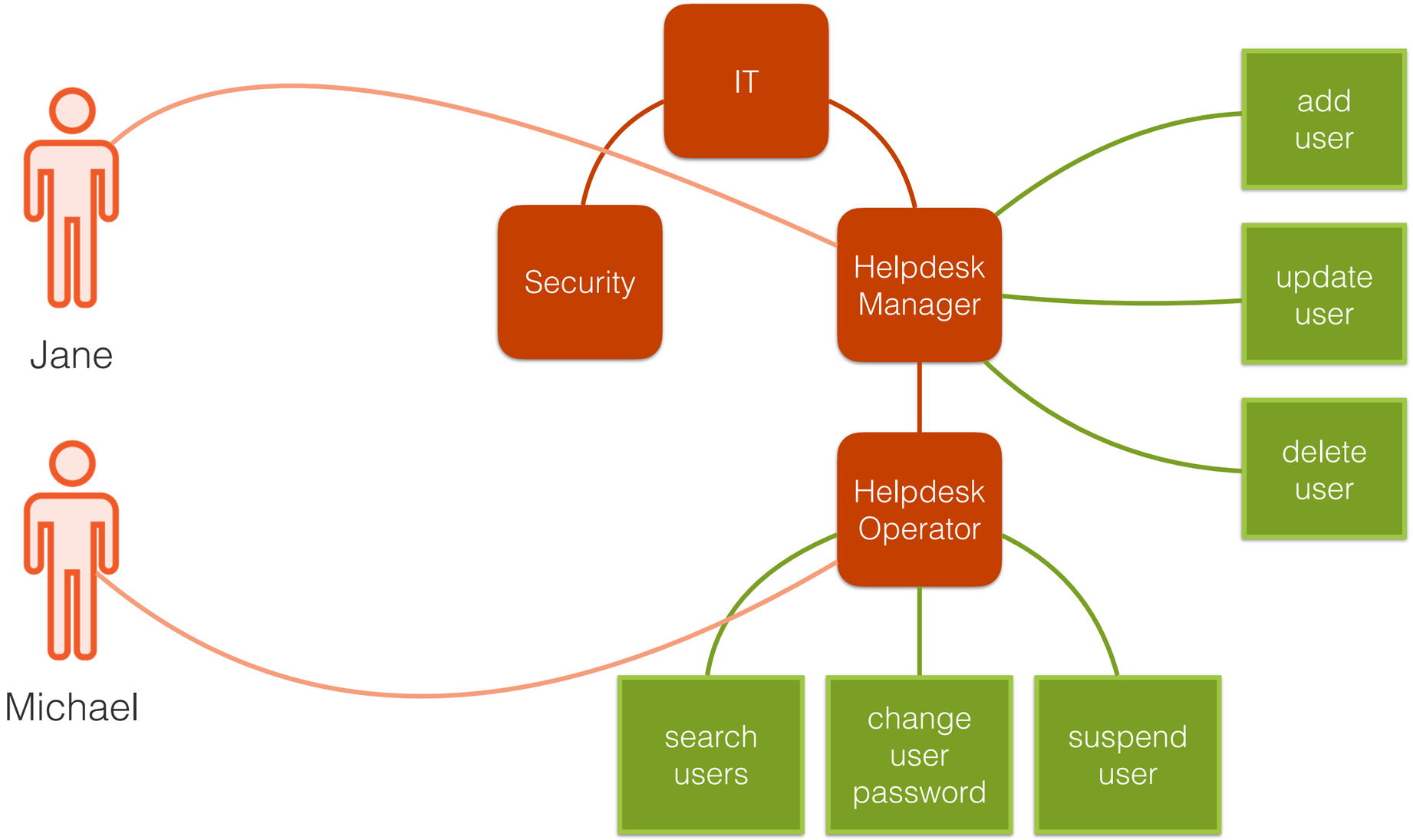
A Theoretical Model



A Theoretical Model



A Theoretical Model



Quick Recap

- Role-based Access Control essentials
- How RBAC is different to ACL
- Saw a theoretical RBAC model

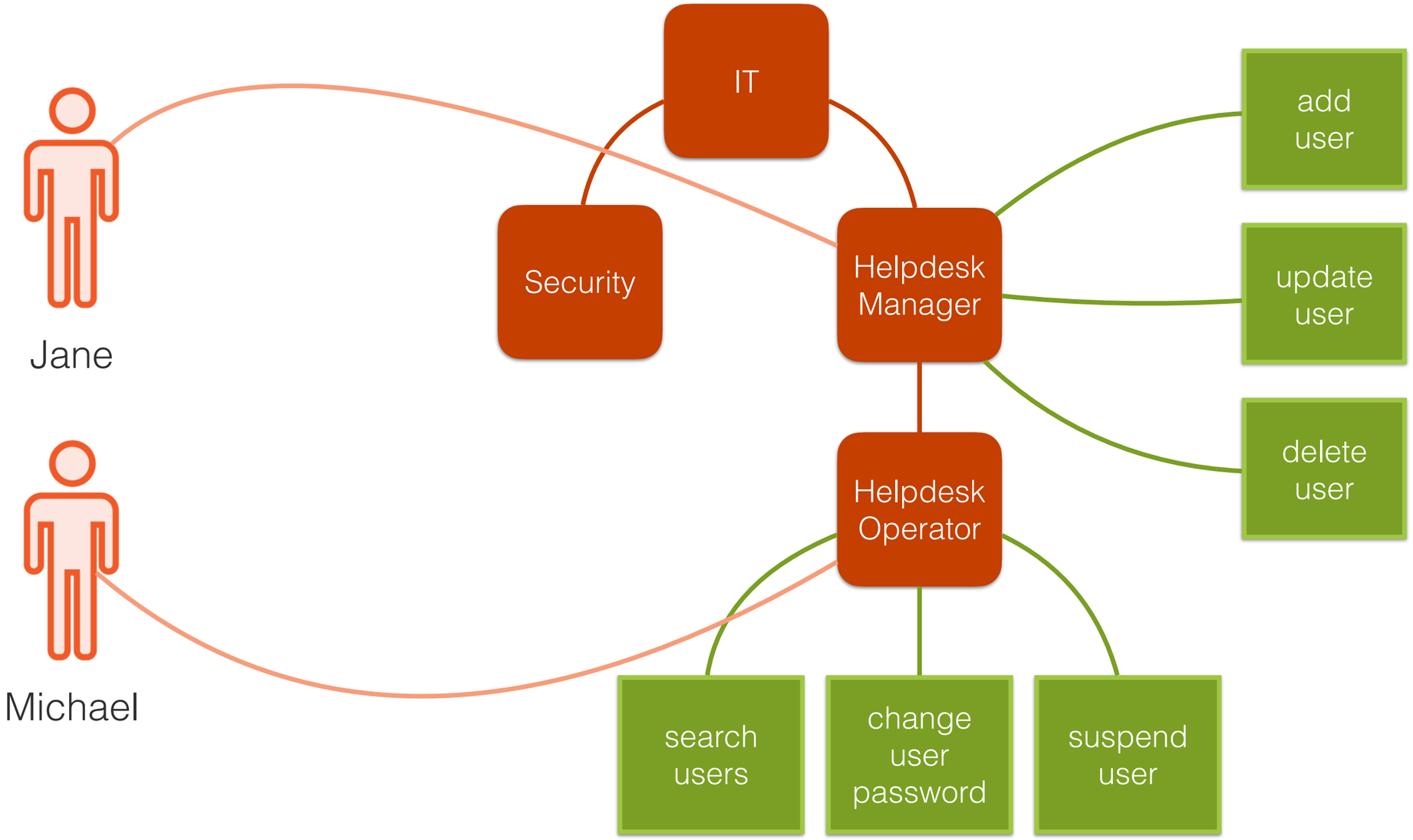
Up Next:
Advantages and Disadvantages

Advantages and Disadvantages

Advantages

- Roles are assigned based on org structure
- Aligns with security principles
- Easier to use and administer than ACLs

A Theoretical Model



Disadvantages

- Users, roles, and permissions need to be well documented
- Users can acquire too many privileges

How to Mitigate RBACs Disadvantages

Conduct Regular Audits

Review Access as Users Change Roles

Quick Recap

- Advantages and disadvantages
- How to mitigate some disadvantages

Up Next:
Implement Role-based Access Control in PHP

Implement Role-based Access Control in PHP

Module Recap

Module Recap

- Learned about Role-based Access Control
- What it is
- How it works
- Advantages and disadvantages
- How to implement it in PHP

Up Next:
JSON Web Tokens