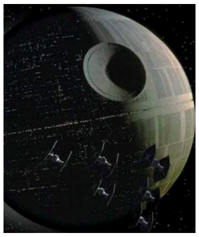
CSci 4271W
Development of Secure Software Systems
Day 2: "What Are We Building?" Diagrams

Stephen McCamant (he/him)
University of Minnesota, Computer Science & Engineering

Based in large part on slides originally by Prof. Nick Hopper

Threat modeling


Star Wars TM and (C) Lucasfilm, Ltd.

- What are we building?
- What could go wrong?
- What are you doing about it?
- How did you do?

What are we building?

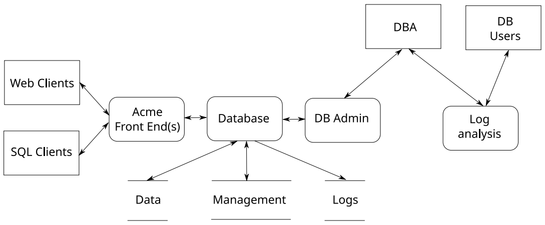
- A good way to start thinking about the security of a system is to start by describing how it works.
- One way to describe a system is to draw a diagram. . .

Outline

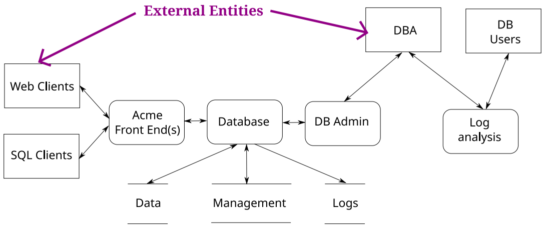
Data-Flow Diagrams

Swim Lane Diagrams

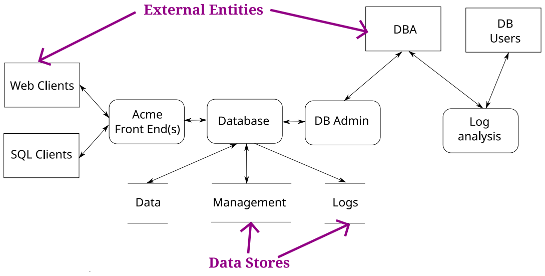
Data-flow Diagrams (DFDs)



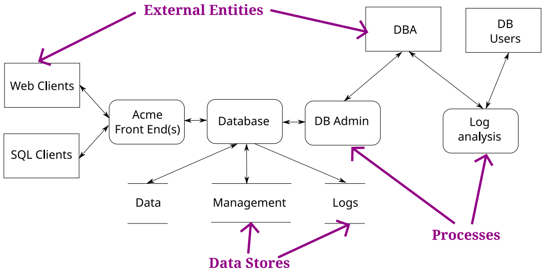
Data-flow Diagrams (DFDs)



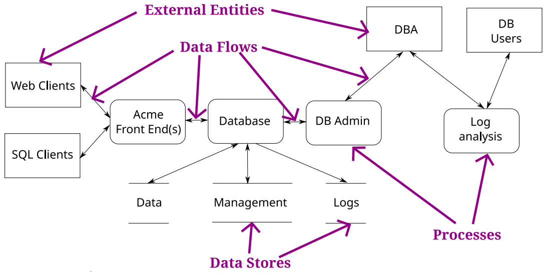
Data-flow Diagrams (DFDs)



Data-flow Diagrams (DFDs)



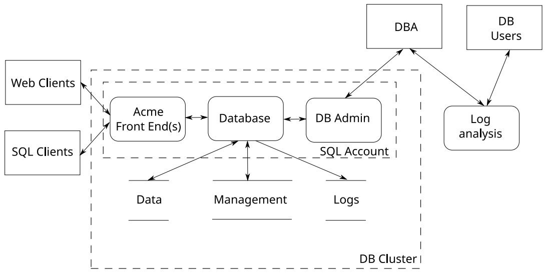
Data-flow Diagrams (DFDs)



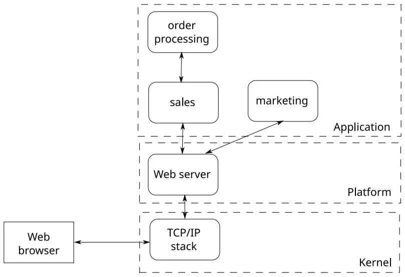
Trust boundaries

- Grouping parts of the system that have mutual trust
- Should encapsulate system "principals":
  - Hosts, UIDs, network segments, . . .

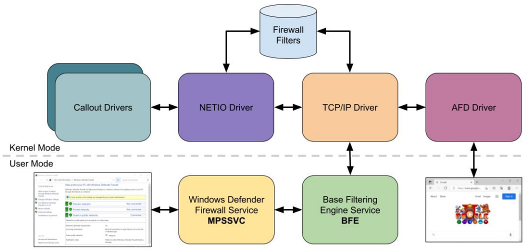
Trust boundaries



More DFD examples

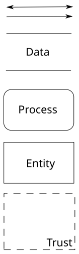


More DFD examples

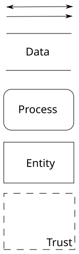


Components implementing the firewall in Windows. Source: Project Zero
`https://googleprojectzero.blogspot.com/2021/08/understanding-network-access-windows-app.html`

Example: GitHub CI



Example: LMS (Canvas, etc.)



DFD guidelines

- Can you describe how the system works with the diagram?
- Are there any data sinks?
- If it's getting too complicated, consider making a sub-diagram
- In what context does process P execute?
- How is access to data store D mediated?

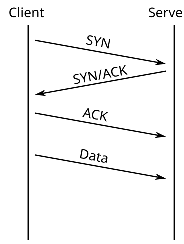
Outline

Data-Flow Diagrams

Swim Lane Diagrams

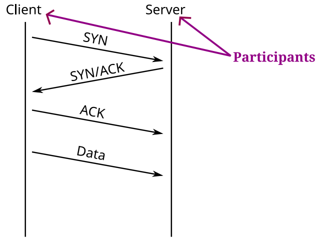
Swim lane diagrams

- Illustrate sequential interactions



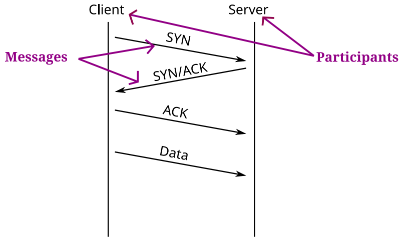
Swim lane diagrams

- Illustrate sequential interactions



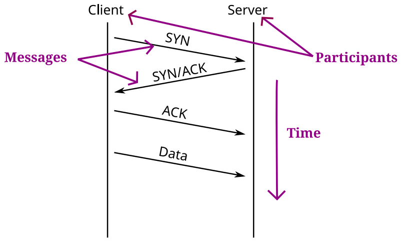
Swim lane diagrams

- Illustrate sequential interactions

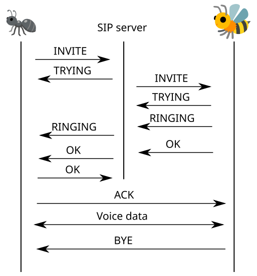


Swim lane diagrams

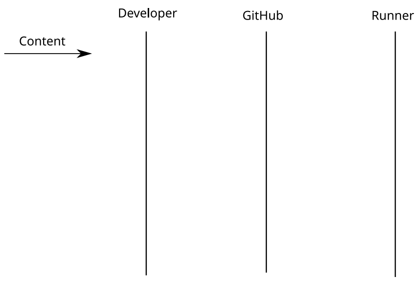
- Illustrate sequential interactions



Another example



GitHub CI swim lanes


Developer
GitHub
Runner
Content