



Privacy and Trust II

Privacy Technology in Context

David Sidi (dsidi@email.arizona.edu)



Administrative things

- Karen Levy on privacy and IPV
- “Chrome is a Google Service that happens to include a Browser Engine”

Goals of threat modeling

- To build a description of threats using an organized process
- The process should help to prevent mistakes and oversights
- *Everything starts with the goals of the project*
 - these should guide the security properties you aim for in your design (what are the assets, which attacks should be handled and which ignored, ...).



What to model

- Assets
- Attackers
- Software



- experts
- less technical input to your project
- prioritization

What to model

- **Assets**
- **Attackers**
- **Software**
- usually: what attackers want, that you want to protect
- Stepping stones really requires understanding attackers and software



Figure 2-2: The overlapping definitions of assets



What to model

- Assets
- Attackers
- Software
- what kinds of attackers do we face?



- Competitor
- Data miner
- Radical activist
- Cyber vandal
- Sensationalist
- Civil activist
- Terrorist
- Anarchist
- Irrational individual
- Government cyber warrior
- Organized criminal
- Corrupt government official
- Legal adversary
- Internal spy
- Government spy
- Thief
- Vendor
- Reckless employee
- Untrained employee
- Information partner
- Disgruntled employee



What to model

- Assets
- Attackers
- Software
- what kinds of attackers do we face?
- A space of attacker features: personas
 1. Identify behavioral variables.
 2. Map interview subjects to behavioral variables.
 3. Identify significant behavior patterns.
 4. Synthesize characteristics and relevant goals.
 5. Check for completeness and redundancy.
 6. Expand descriptions of attributes and behaviors.
 7. Designate persona types.



What to model

- Assets
- Attackers
- Software
- what kinds of attackers do we face?
- A space of attacker features: personas
- what will the attacker do?
 - problems with bias



What to model

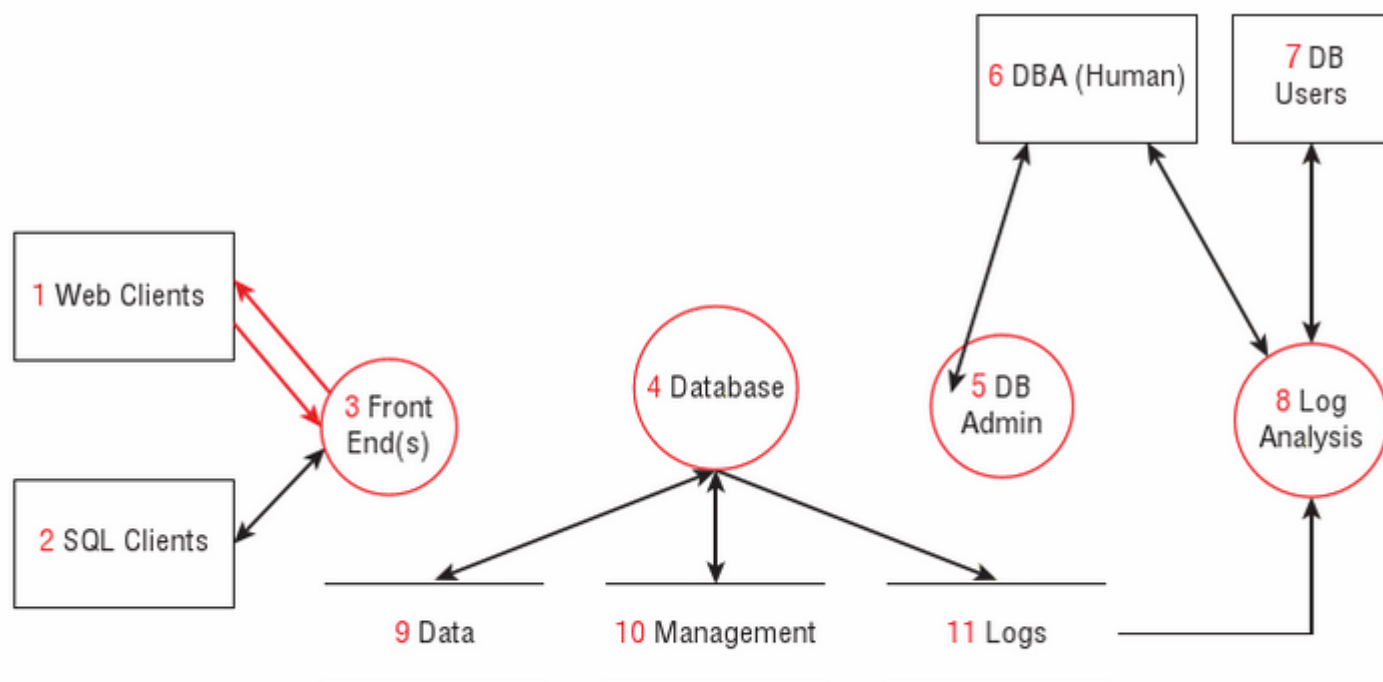
- Assets
- Attackers
- Software
- modeling software in a way that helps to unearth threats



Learn you diagramming for great good!

- Point is to diagram how the system works
- Done in a group with a wide variety of people (you want them to turn out to be across trust boundaries): if there is disagreement, this usually means a security problem is nearby

Data flow diagrams



Key:

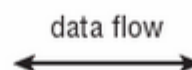
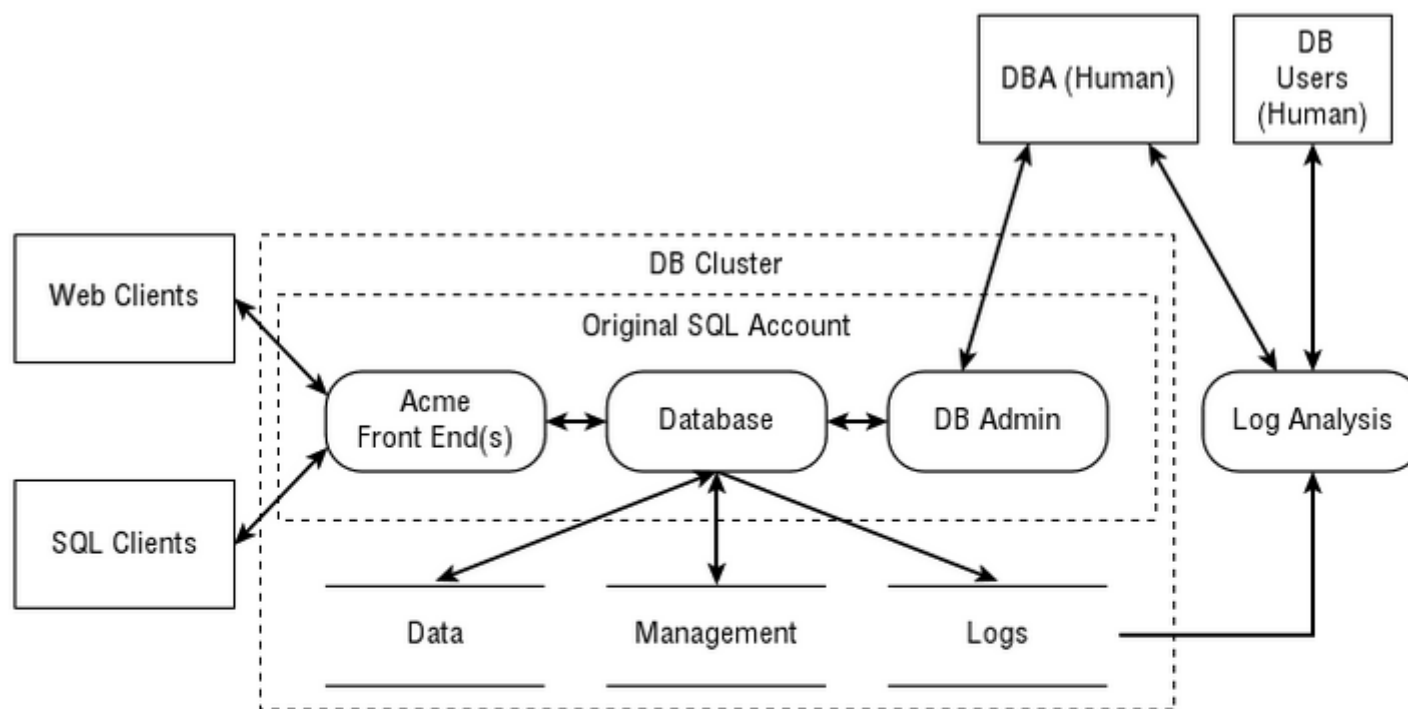


Figure 2-3: A classic DFD model

Data flow diagrams



Key:



Figure 2-4: A modern DFD model (previously shown as Figure 2-1)

Swim lane diagrams

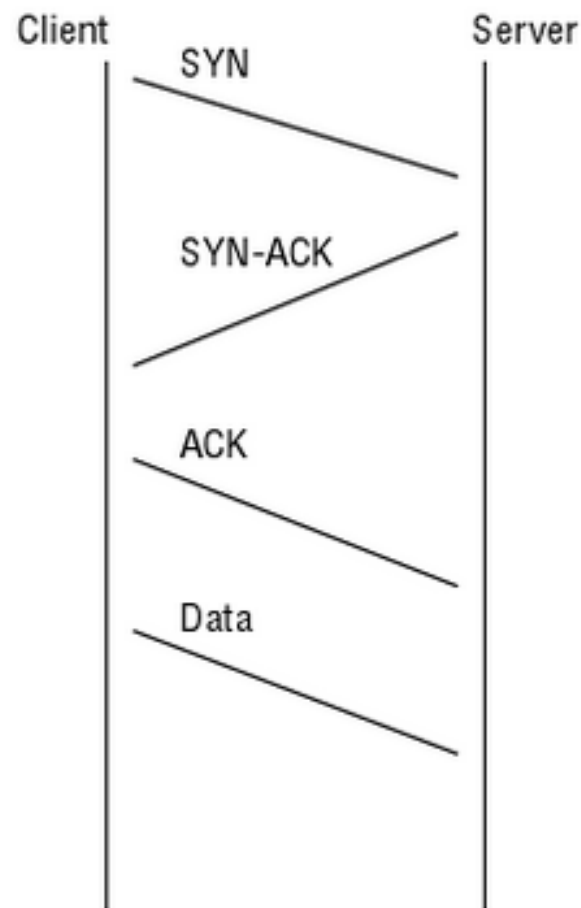
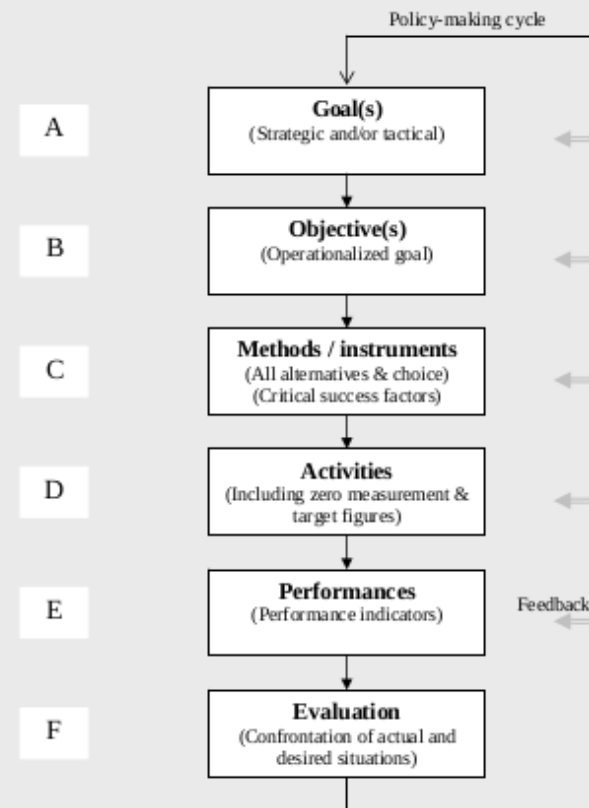


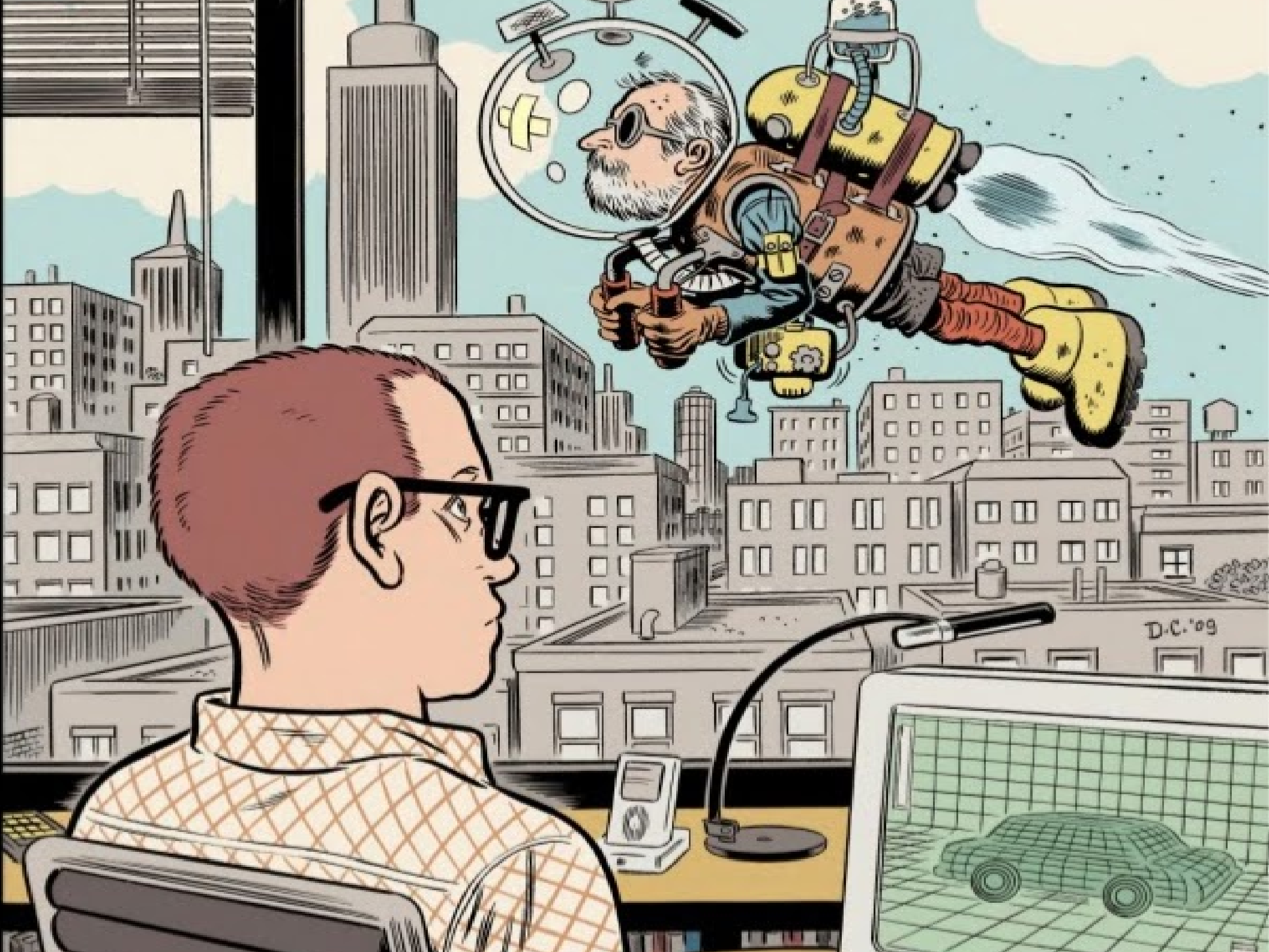
Figure 2-6: Swim lane diagram (showing the start of a TCP connection)

One thing Shostack misses

- Threat modeling is an ongoing process
- Like any policy, it should be under constant evaluation, and subject to revision
- Such revision should be part of the plan for early in the project's development

Figure 1: Basic framework – the six steps of the policy-making cycle¹







For the rest of the class, we will work on threat modeling hands-on

- Assignment 3 description (see wiki)
- In groups, and recording things as you go, start to address the design part of the assignment for your chosen topic. I will circulate