COLLEGE OF SOCIAL & BEHAVIORAL SCIENCES
School of Information

Privacy and Trust

Privacy Technology in Context

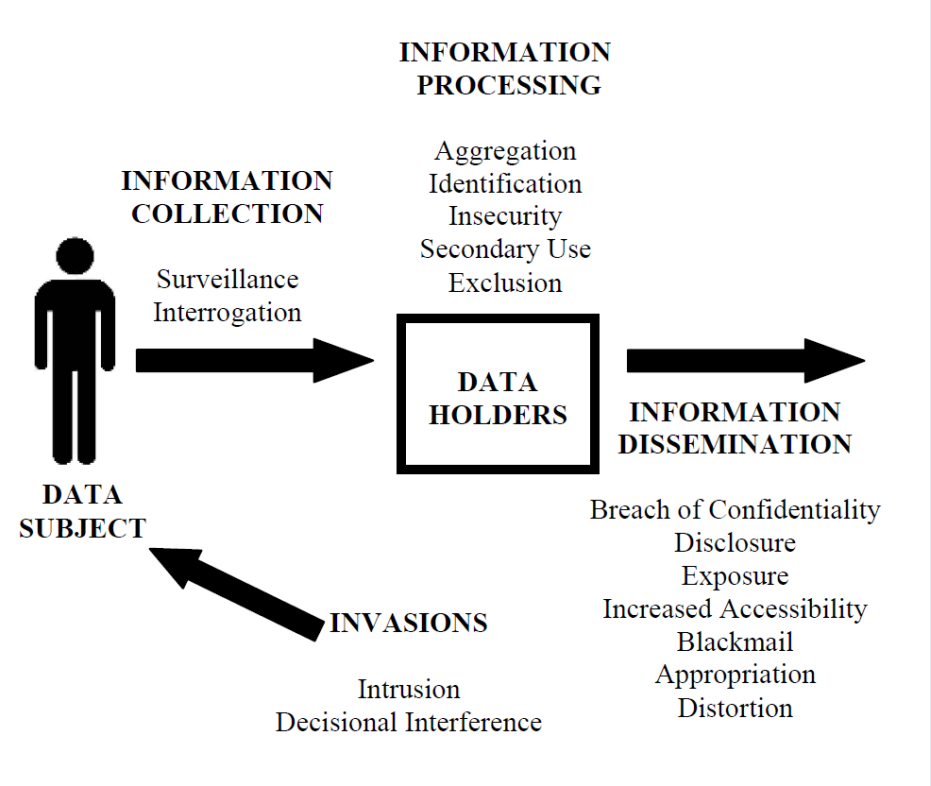
David Sidi (dsidi@email.arizona.edu)

Administrative things

- Explanation for challenge 2
- Why we are doing this module now
  - Final project proposals

Privacy and Harm

- One view: Information privacy is best understood by thinking about characteristic privacy harms
- Privacy technologists who subscribe to this view aim to design and implement technologies to reduce these harms.
- This brings privacy research closer to security research
- See: Danezis, Solove, many more



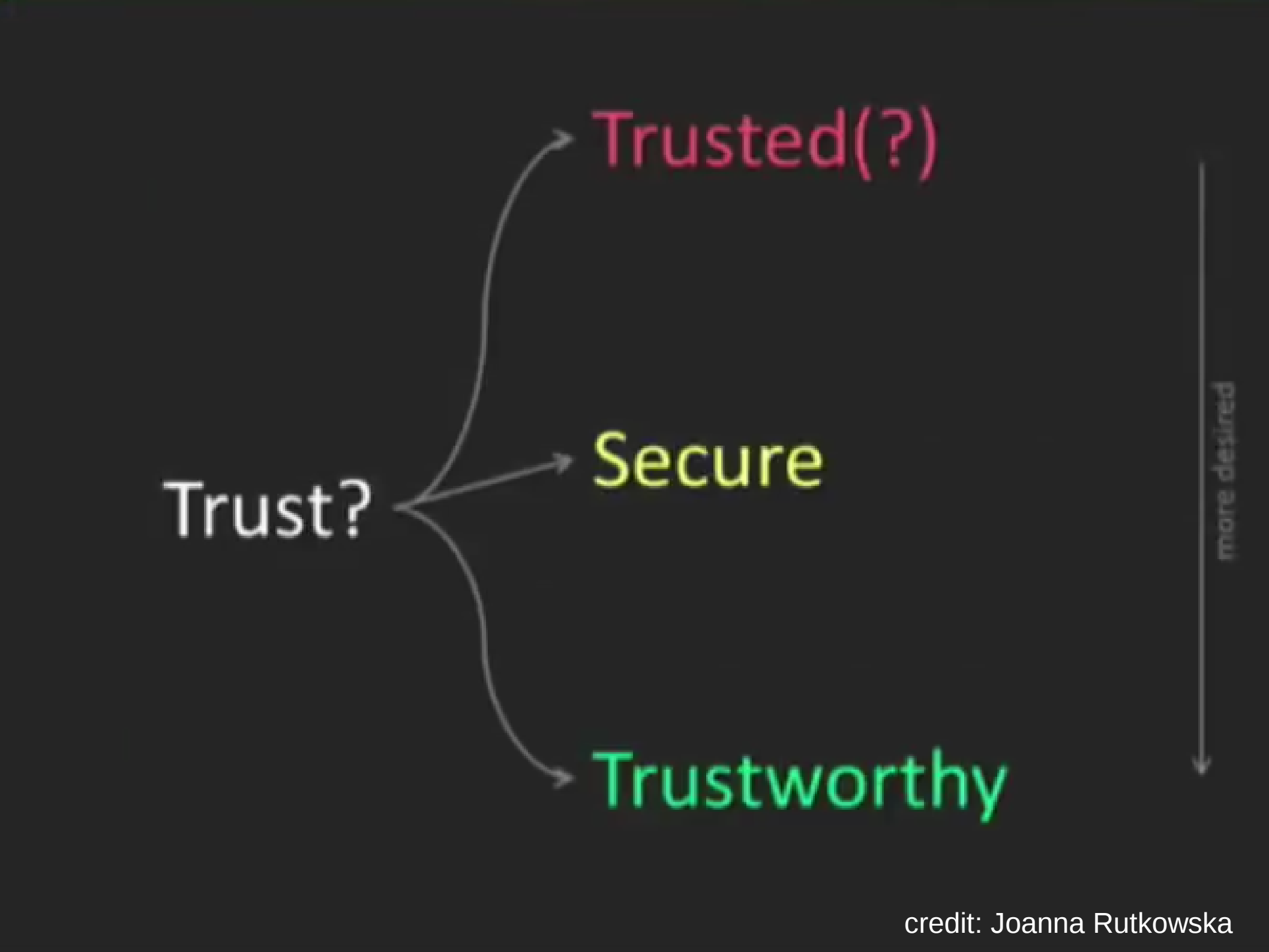
Example harms to information privacy

- A newspaper reports the name of a rape victim.
- An abusive spouse installs an app to surveil his wife
- A state government intercepts communications between a journalist and a source.
- Cameras arranged in a city downtown are able to identify and track the movements of everyone who passes, and store the information indefinitely
- Reporters gain entry to a person's home and secretly photograph and record the person without that person's knowledge.

- New X-ray devices can see through people's clothing
- A company markets a list of five million elderly incontinent women.
- A company links publicly available records with aggregated private records to reveal sensitive medical information
- A company suffers a breach and leaks millions of social security numbers linked to names, addresses ad more information
- Despite promising not to sell its members' personal information to others, a company does so anyway.
- A government collects all internet traffic originating or passing through its country, promising not to analyze it unless there is a need at a later date.

Example PETs for these harms

- Maintaining aliases, name changes
- PGP, OTR, Conversations
- Privacy Visor, Glamouflage
- Bowley Locks
- (Buy a backscatter x ray machine) Request a pat down
- Spamgourmet, Random Agent Spoofer, cash payments, sharing affinity cards
- Fingerprint marking
- Tor, I2P, TLS (not great...)



credit: Joanna Rutkowska


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Definitions of trust

- an assumption in a model of a system which, if false, breaks the security policy for the system (NSA definition)
- a system “whose integrity cannot be assured by external observation of its behaviour whilst in operation” (Ross Anderson, attributed as “a UK military view”)

Privacy and Benefit

- An alternative to focusing on harms
- Friedman on Value Sensitive Design: there are benefits to be had by working to achieve privacy without minimizing trust; trust can be valuable
  - video (@ 20:03)
- Technology can have a role in fostering trustworthiness
- Also: you're stuck with trust in the use of privacy technology, as we'll see in a very clearly specifiable way

Today, we focus on identifying, preventing, mitigating, and recovering from privacy harms with threat modeling (future classes will focus on the benefits view)

Goals of threat modeling

- To build a description of threats using an organized process
- The process should help to prevent mistakes and oversights

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

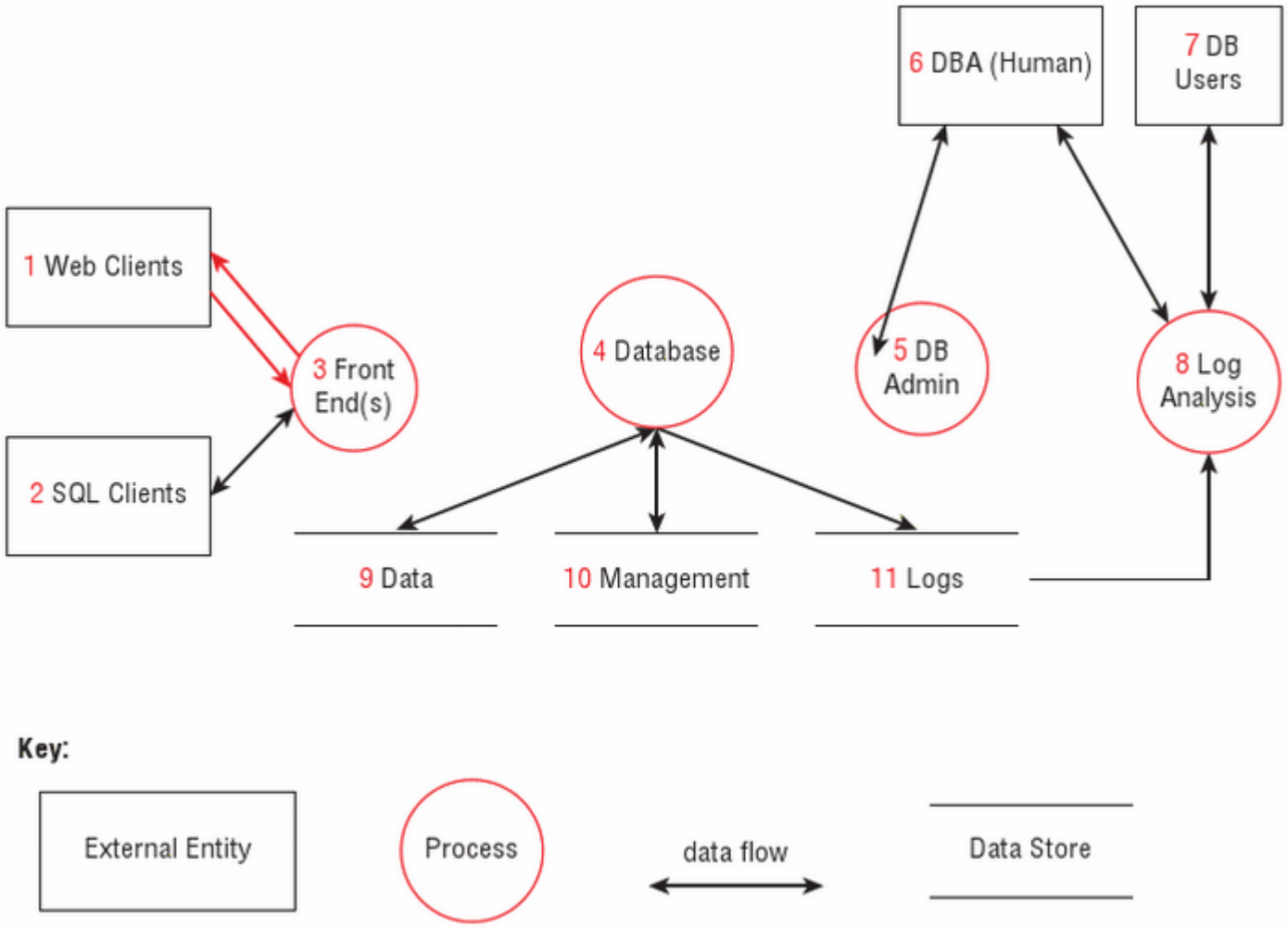


Figure 2-3: A classic DFD model

Data flow diagrams

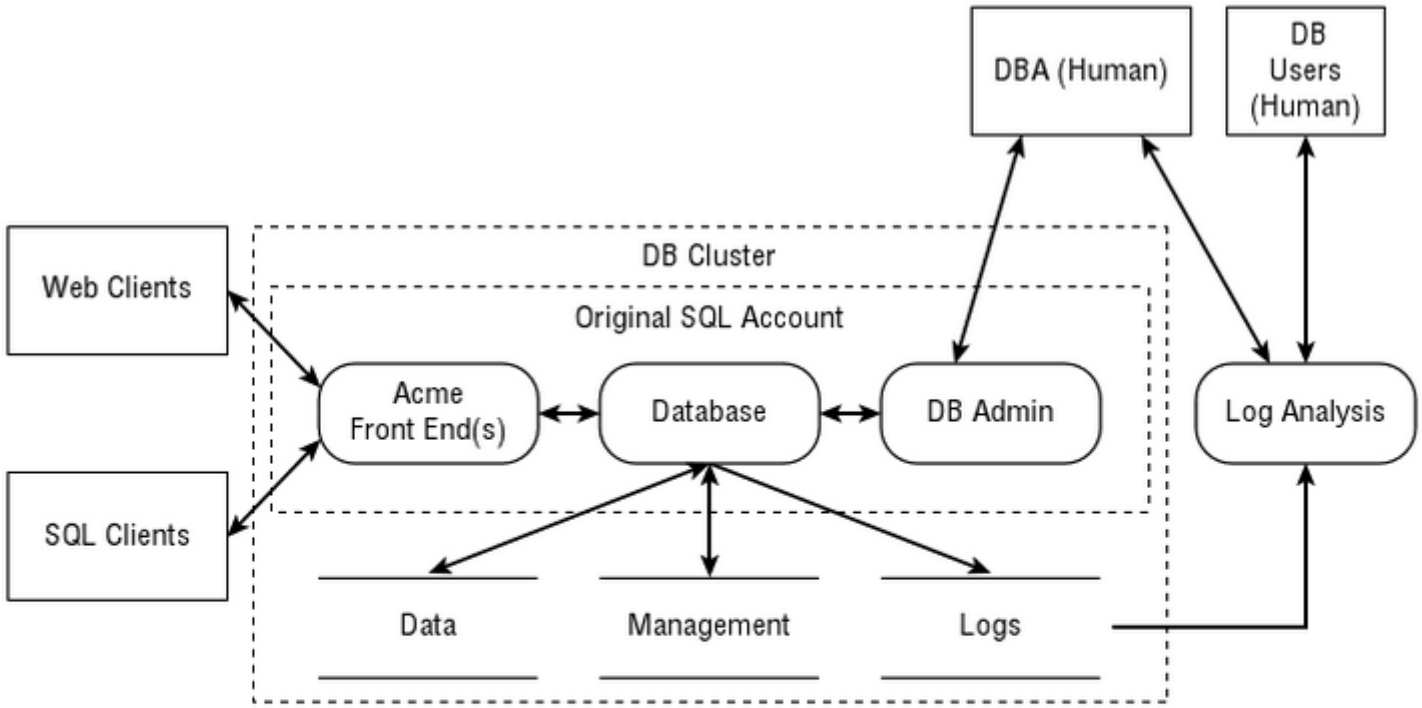


Figure 2-4: A modern DFD model (previously shown as Figure 2-1)

Swim lane diagrams

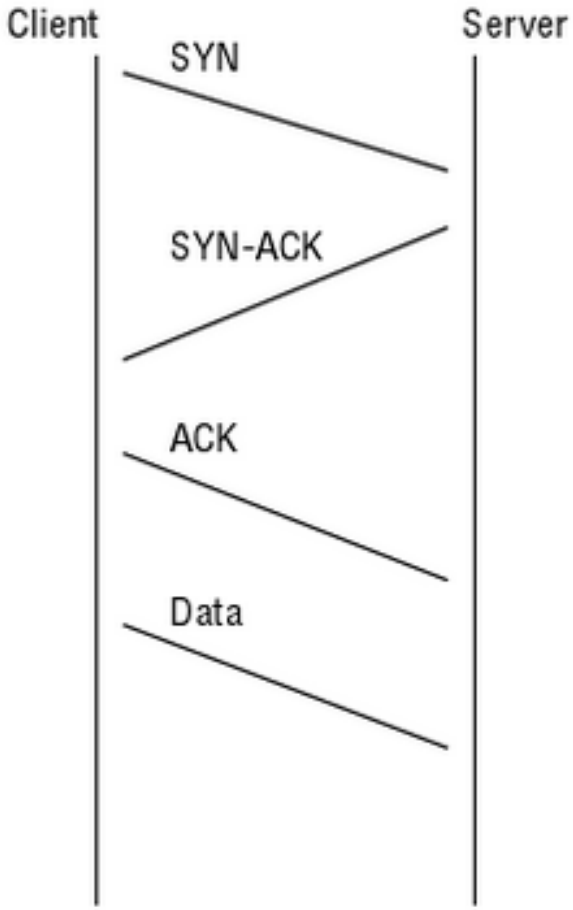


Figure 2-6: Swim lane diagram (showing the start of a TCP connection)