

ECE750: Usable Security and Privacy

Social Media – Mental Models

Dr. Kami Vaniea
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca



UNIVERSITY OF
WATERLOO

FACULTY OF
ENGINEERING



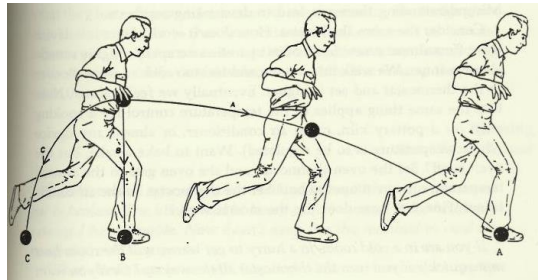
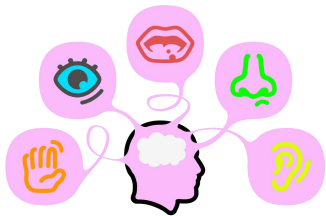
First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
 1. Some students show up late for various good reasons
 2. Reward students who show up on time
 3. Important to see real world examples

MENTAL MODELS

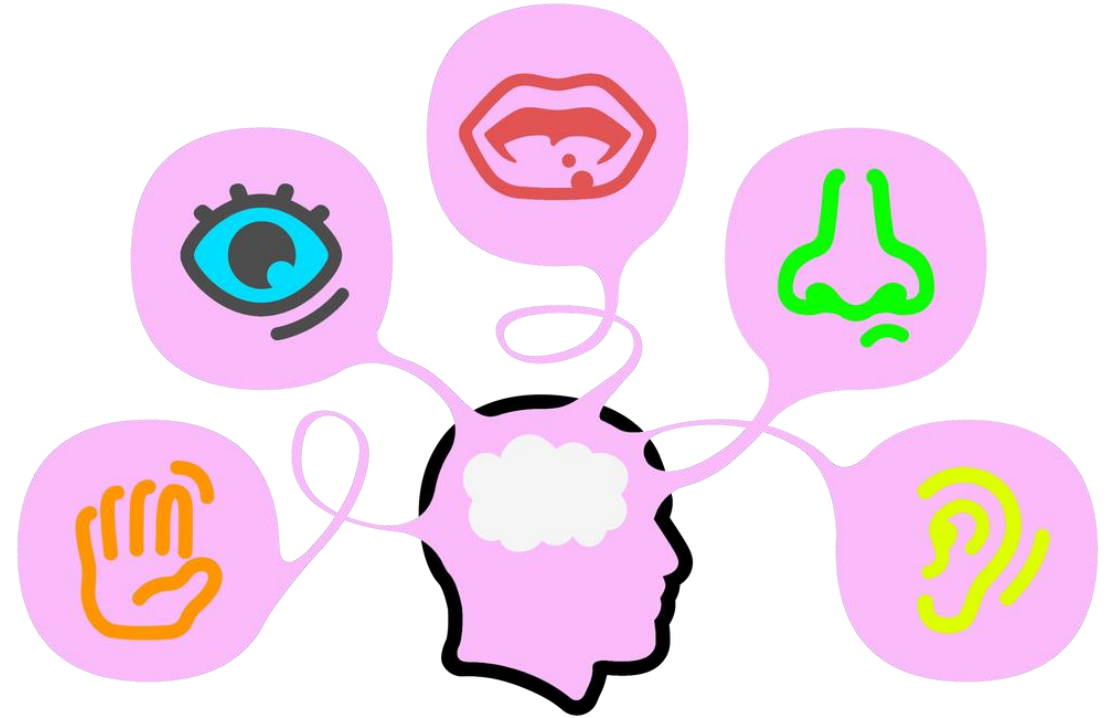
I'm going to:

- Talk about how your brain works
- What that means for how humans interact with technology.
- The types of skills we are going to teach you in this class that help you use, rather than fight, how all our brains work.



Your brain can't actually "see" the world

- Your brain is trapped in a skull.
- It has five senses connected to it that feed in data.
- It uses the senses to gather information about the world.
- It uses those senses, along with memory, to construct an understanding of what the world looks like.



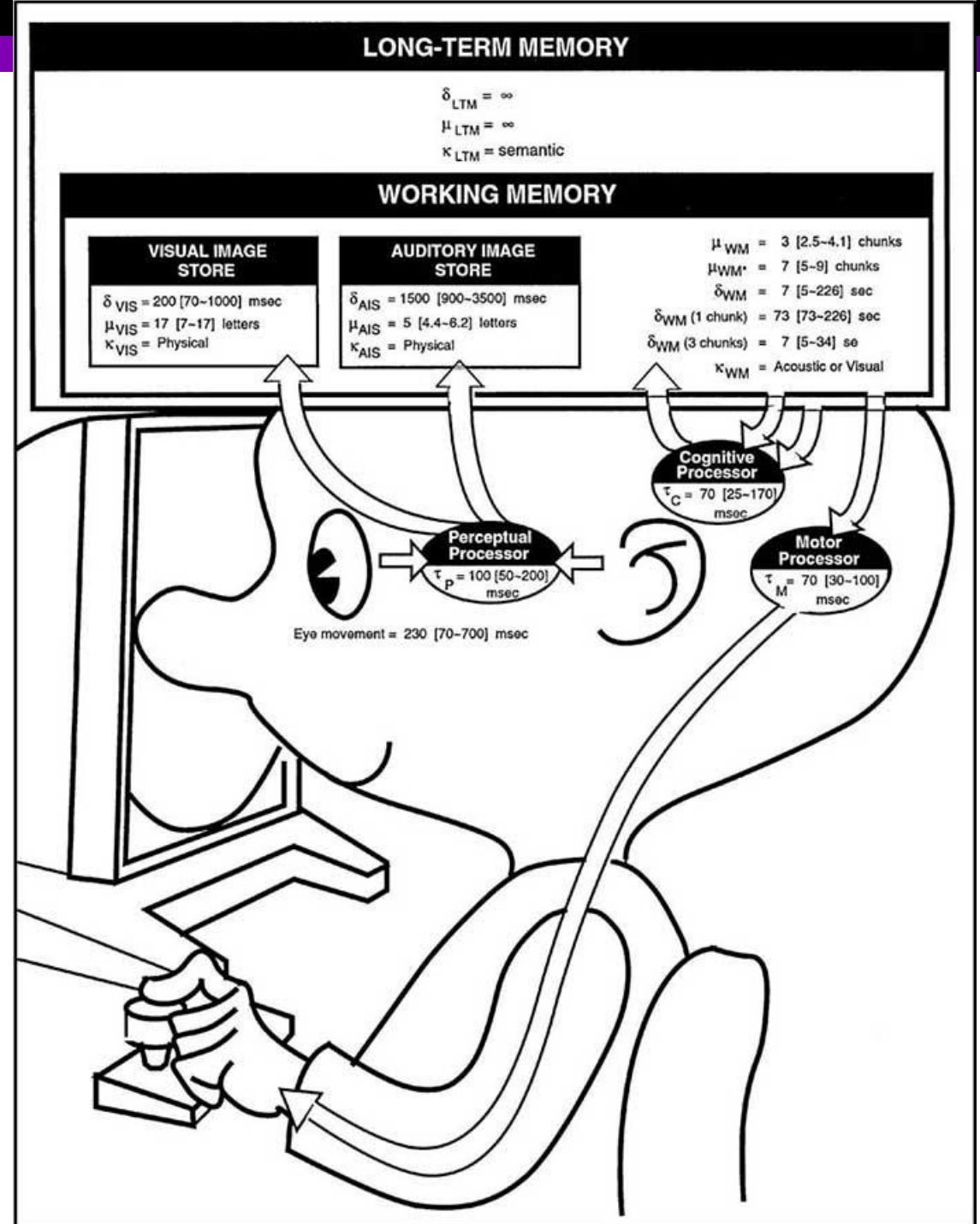
Your brain can't actually "see" the world

- Your brain is trapped in a skull.
- It has five senses connected to it that feed in data.
- It uses the senses to gather information about the world.
- It uses those senses, along with memory, to construct an understanding of what the world looks like.



Processing data also takes time

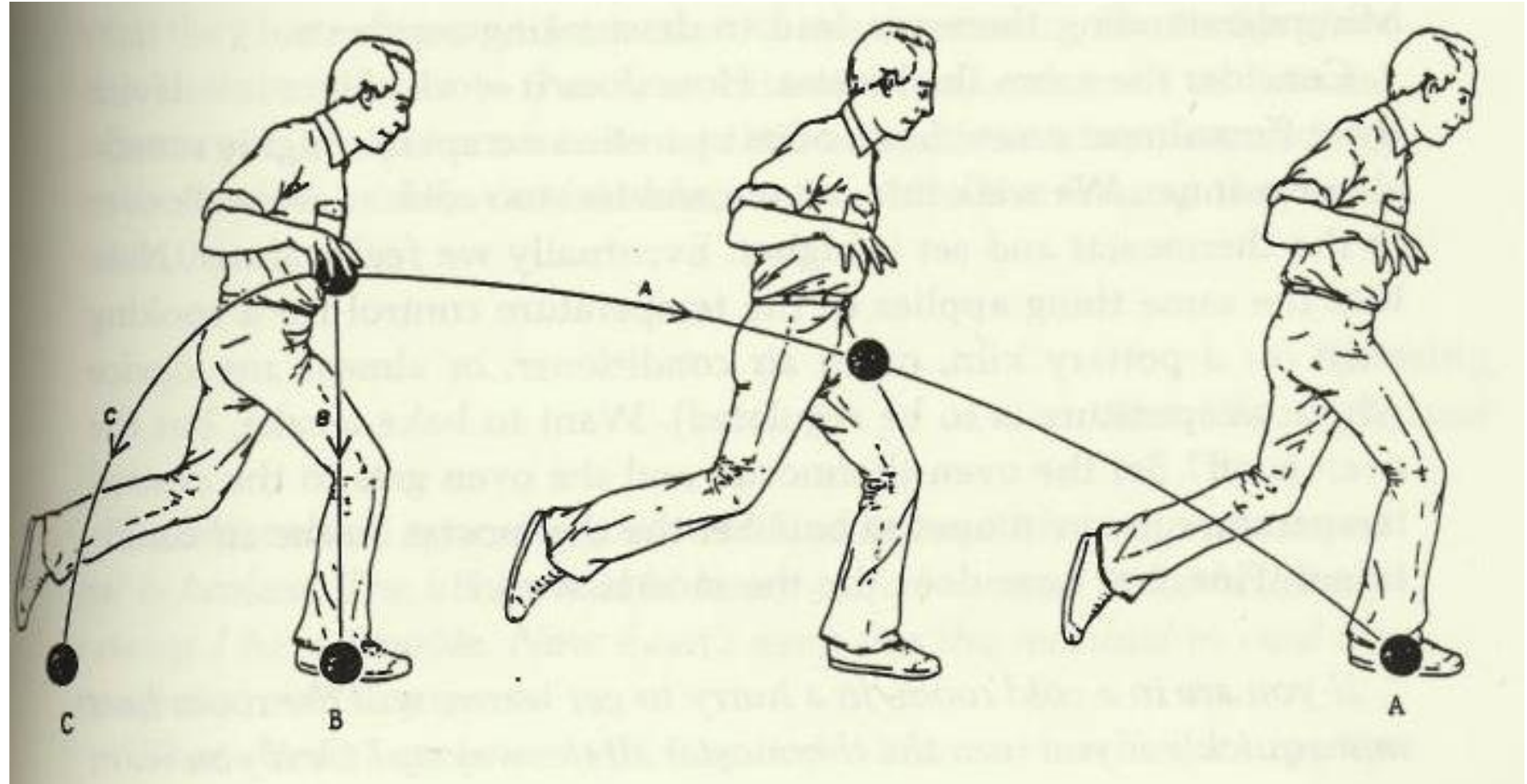
- Your brain is very fast, but it cannot process data instantly.
- So it builds a “mental model” that lets it reason about not only the present but also the future.
- This model is strongly biased by past experiences and memories.
- It also takes into account the brain’s own processing time.





Mental models:

If the man drops the ball while running, what path will it take?



Your brain builds models and then uses them to make very fast decisions about the world.

5
E₁

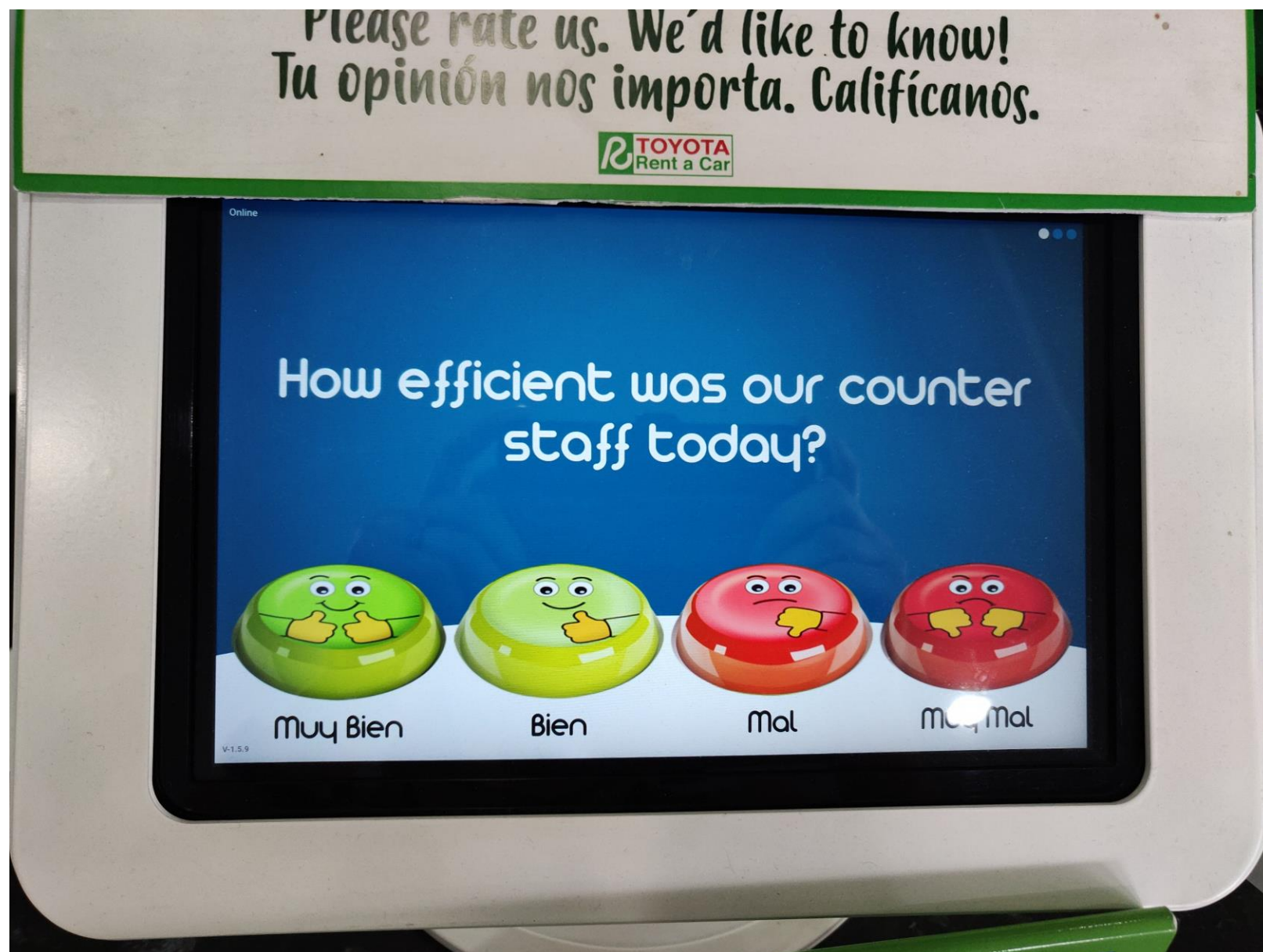
PULL



PUSH



Good design supports fast thinking and allows users to interact without reading.



Good design supports fast thinking and allows users to interact without reading.

AMERICAN EXPRESS

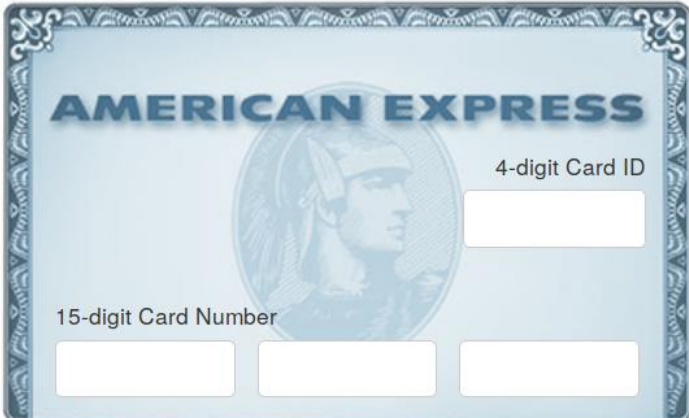
1. Get Started

2. Set Up

3. Finish

Welcome!
Let's get started

Please enter your Card details to begin.

A graphic of an American Express card is centered on the screen. The card is light blue with a dark blue border. It features the 'AMERICAN EXPRESS' logo at the top, a circular emblem with a profile of a person in the center, and two input fields at the bottom. The top input field is labeled '4-digit Card ID' and the bottom input field is labeled '15-digit Card Number'.

AMERICAN EXPRESS

4-digit Card ID

15-digit Card Number

Confirm

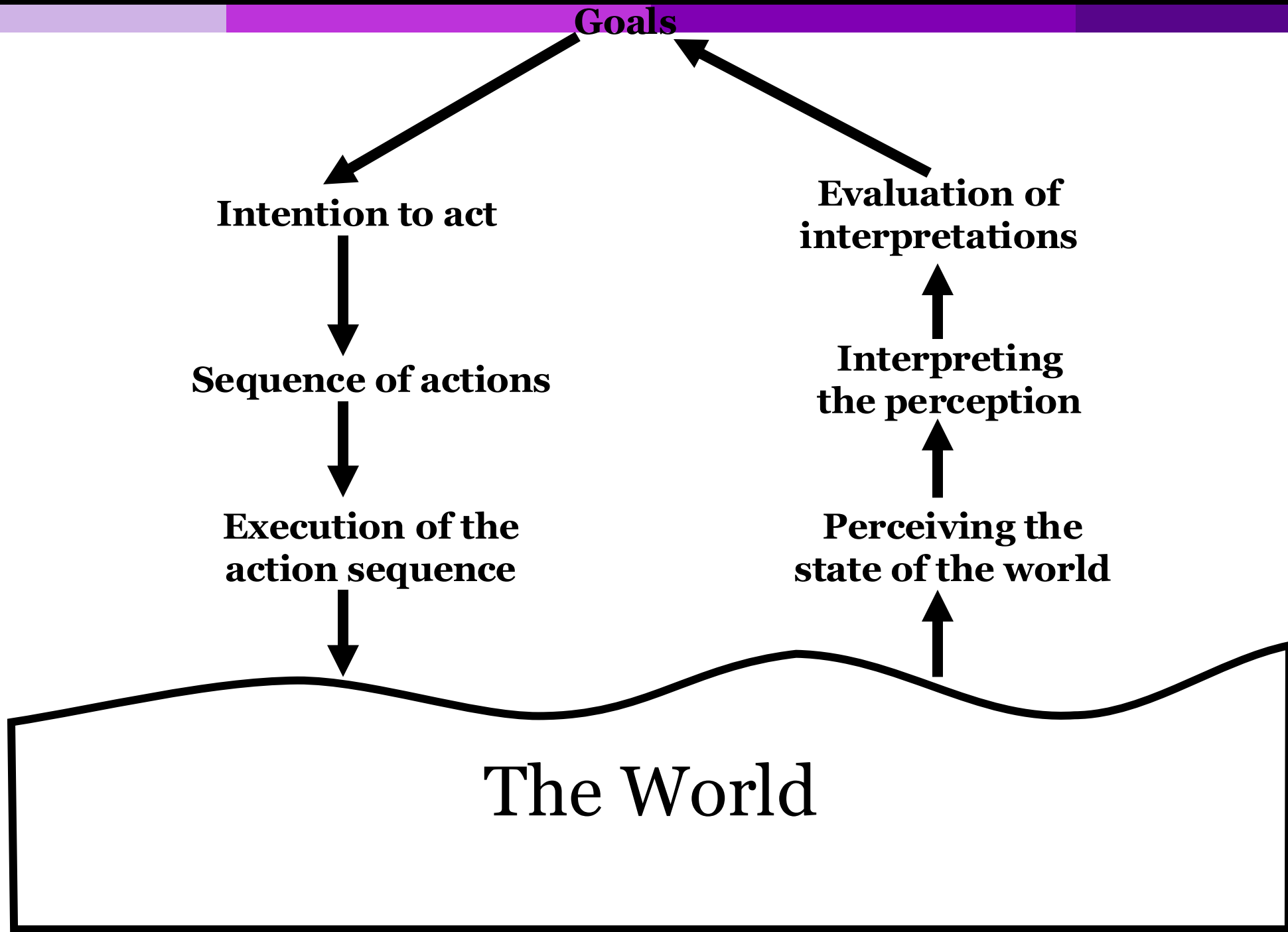
The problem

- Most people in this class are digital natives.
- Your brains have been trained to process user interfaces FAST.
- Good HCI designers have learned how to:
 - Slow down.
 - Think about how others will process.
 - Think about why something is hard to use.
 - Design so that other people can do fast interaction.



“A user interface is well designed when the program behaves just as the user thought it would.”

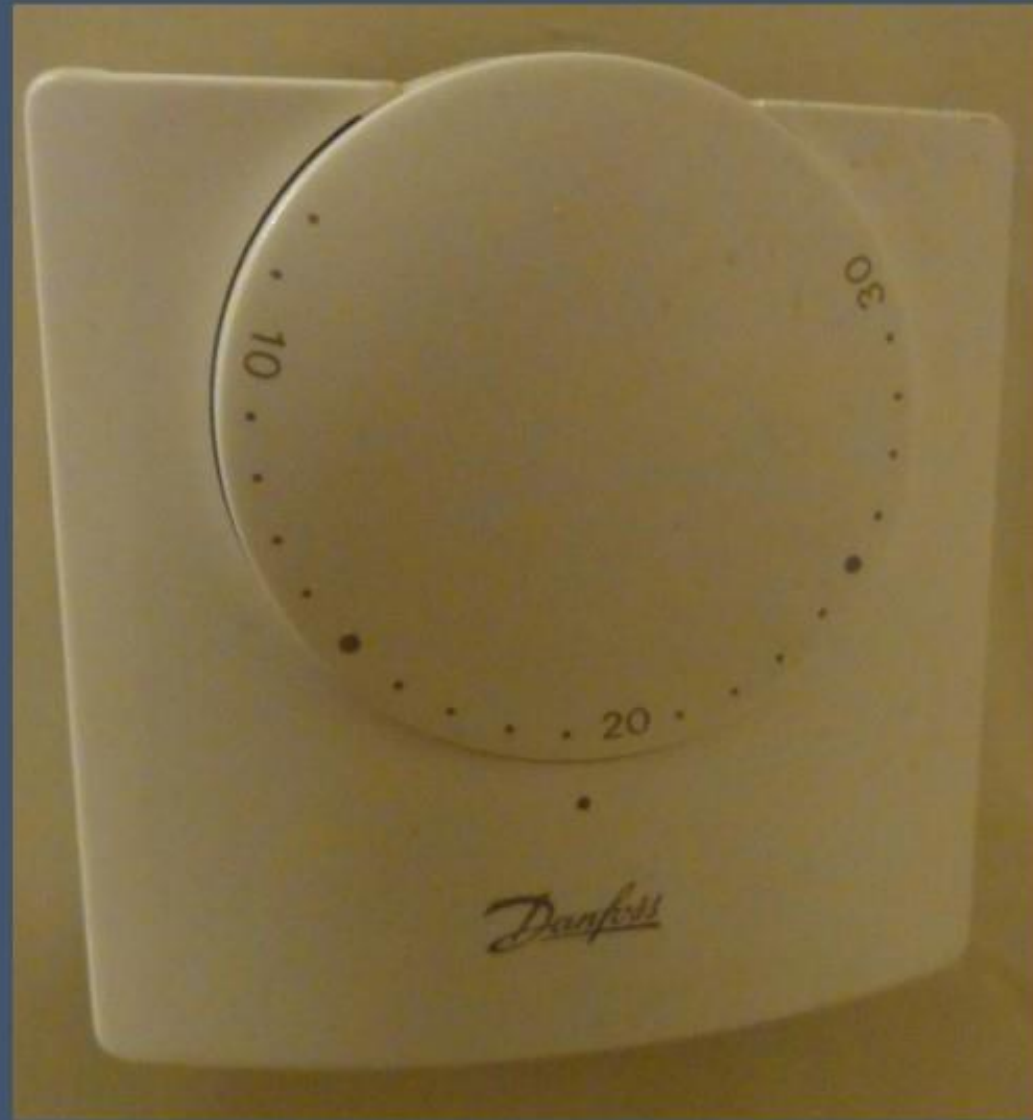
-- Joel Spolsky



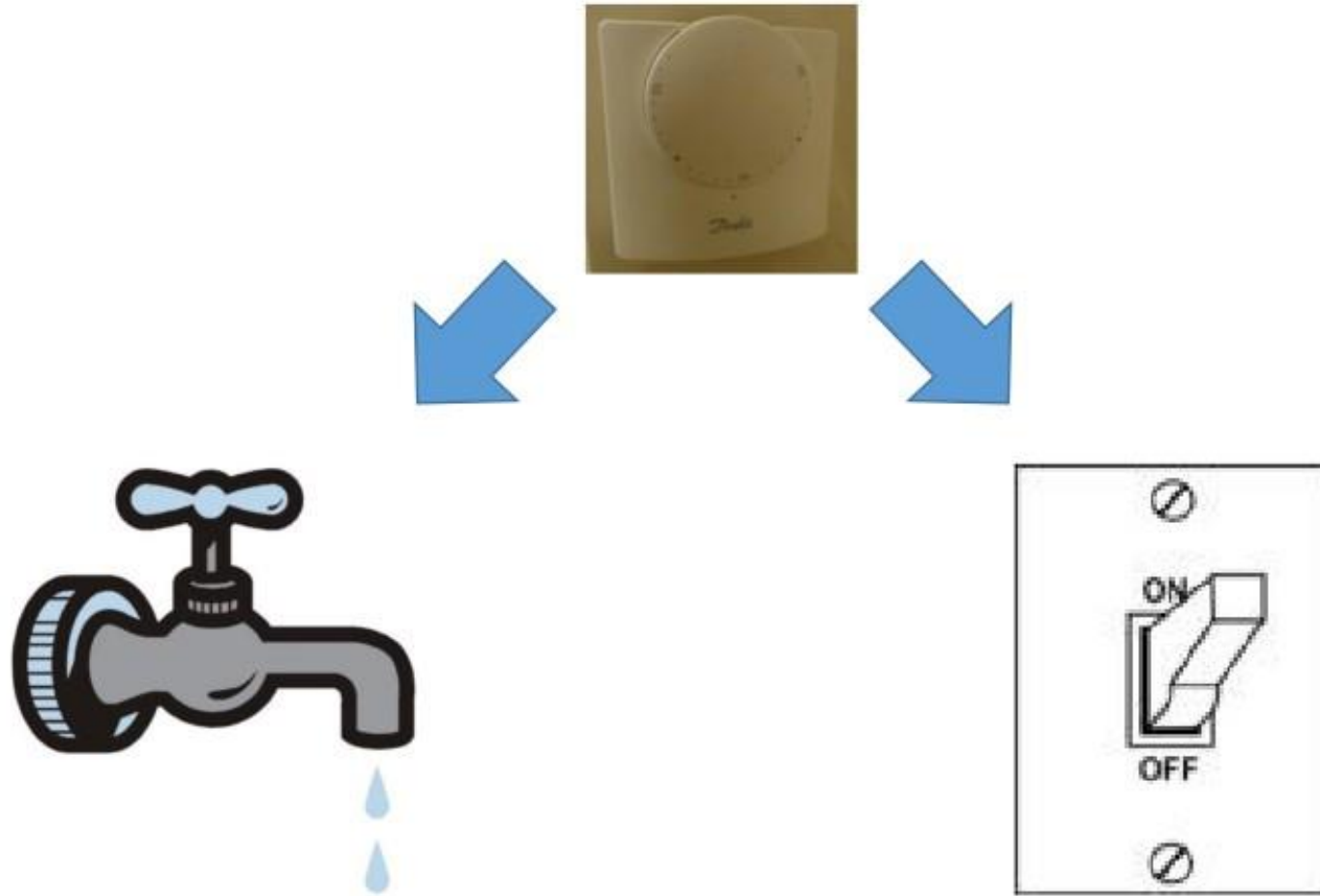
The heating has just come on but the room is cold. The room thermostat is set where you normally have it (higher than the current room temperature).

Do you...

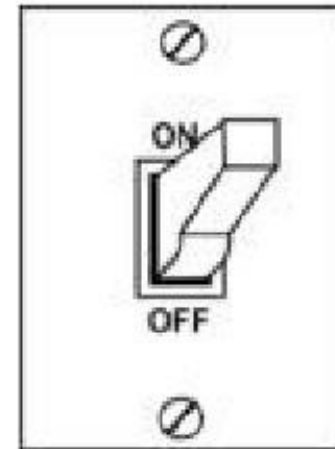
1. Turn it up so the room heats faster
2. Leave it where it is and just wait?



Do room thermostats work like taps or switches?

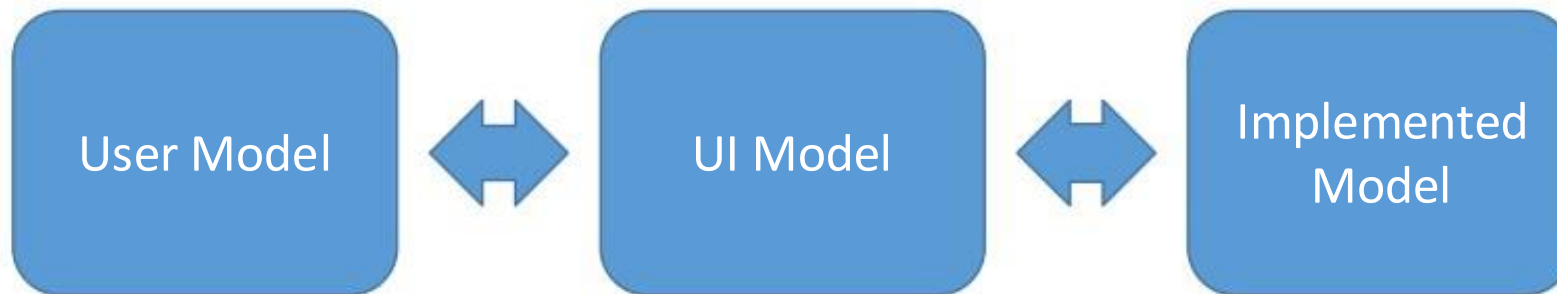


Do room thermostats work like taps or switches?

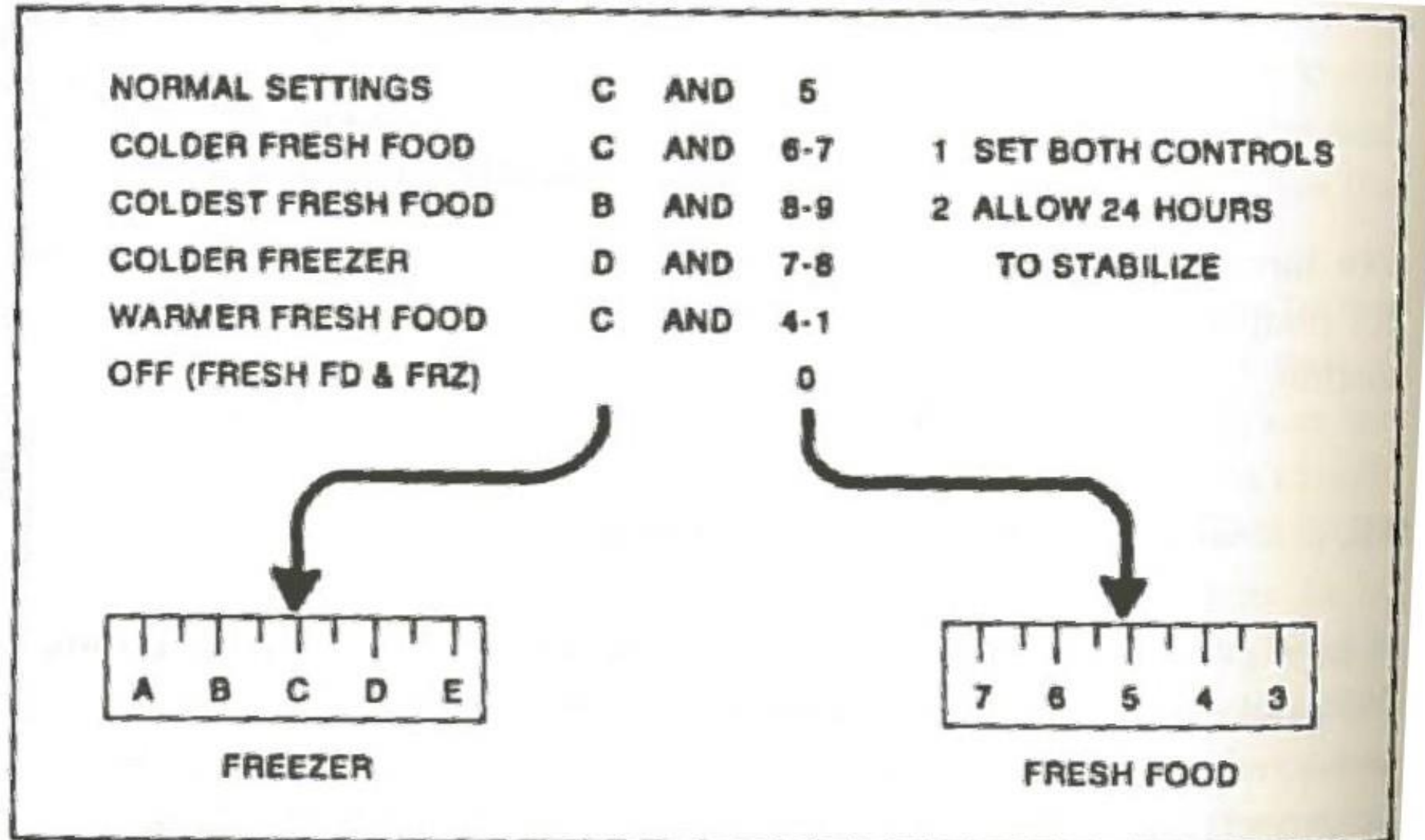


There are three models of the system

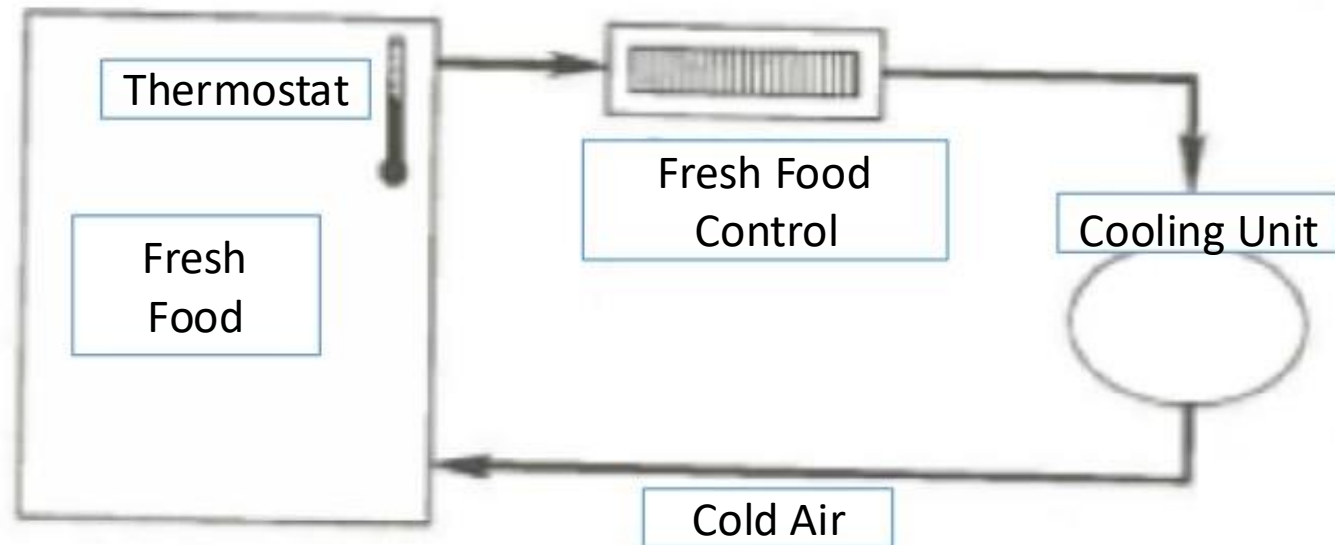
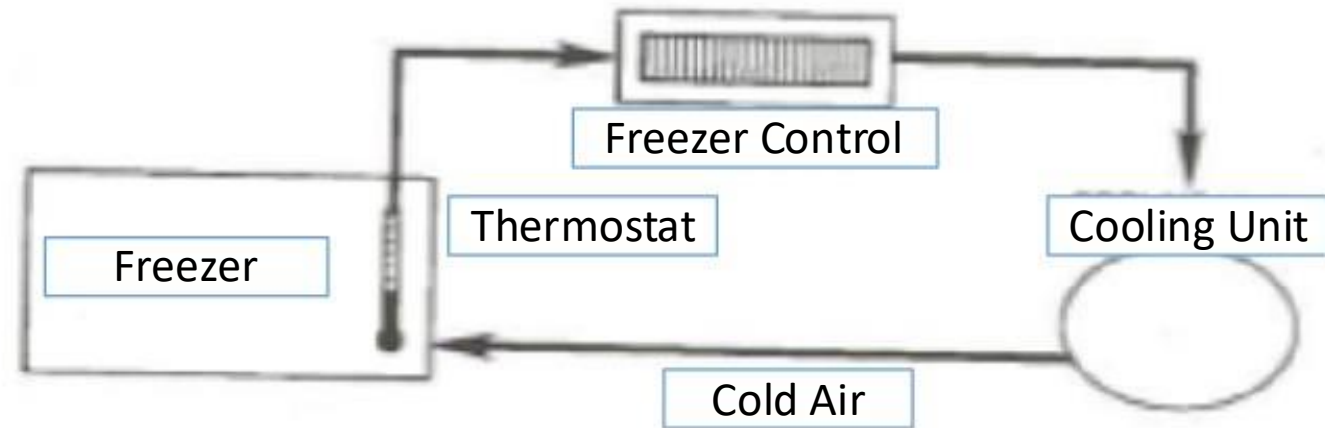
- User Model - How the user thinks the product works. The mental model.
- UI Model - How the product is presented to the user in the user interface.
- Implementation Model - How the product is actually implemented.



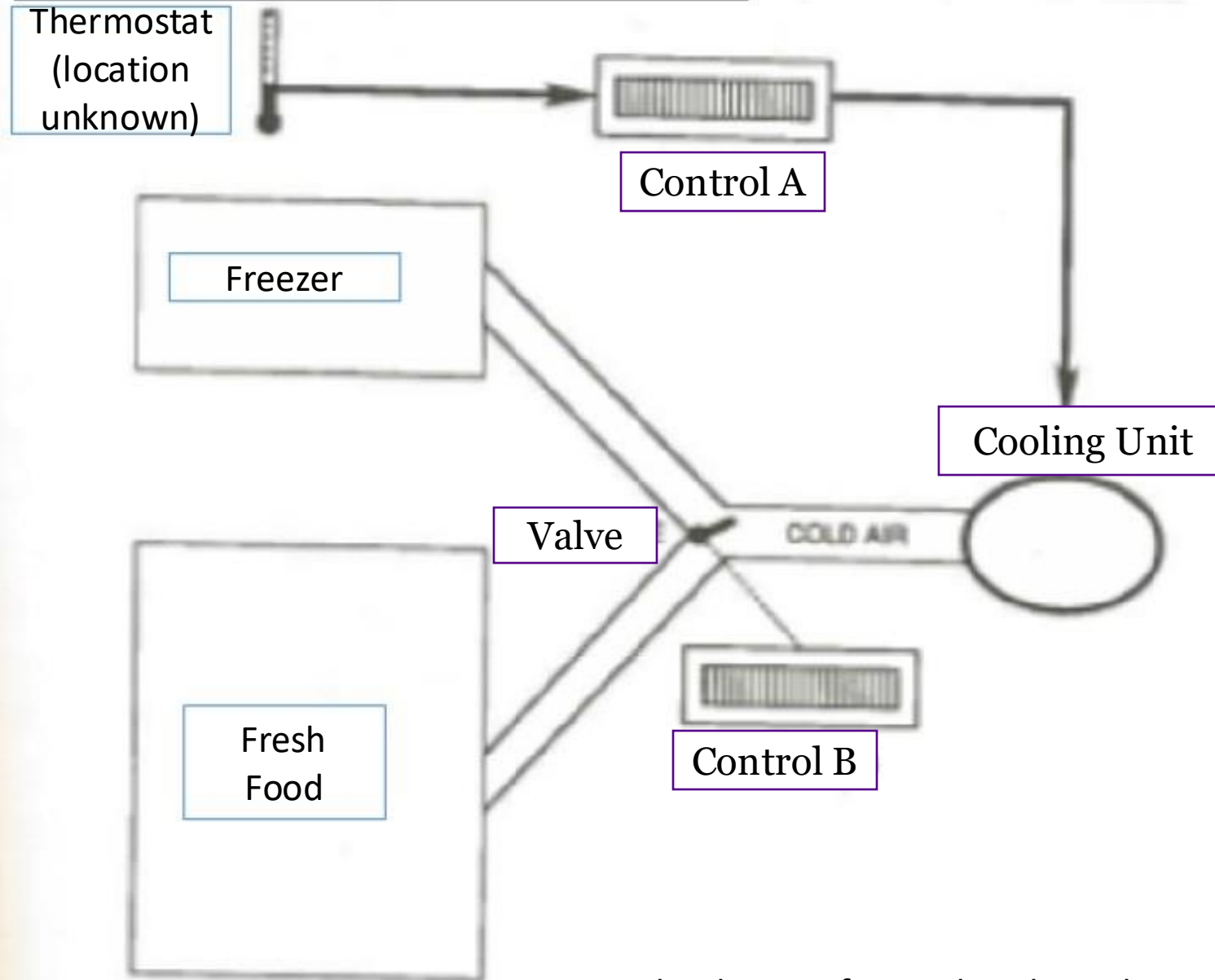
UI Model (refrigerator temperature)



User mental model



Implemented model

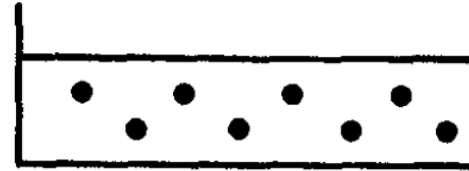


Good user interfaces help the user develop a good mental model of the system.

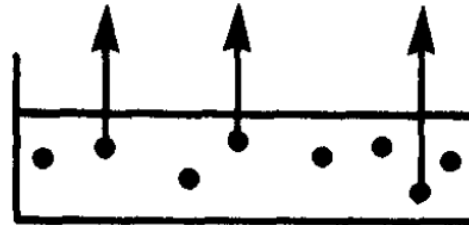
How do we learn about the mental models people have?

Mental models of water evaporation

Heat Threshold Model

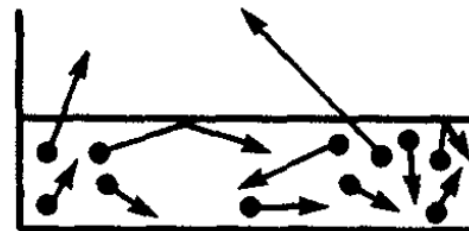


BELOW-BOILING



ABOVE-BOILING

Rocketship Model



Mental models of water evaporation



Table 10.4. *Evaporation questions*

Question 1. Which is heavier, a quart container full of water or a quart container full of steam?

Question 2. Why can you see your breath on a cold day?

Question 3. If you put a thin layer of oil on a lake, would you increase, decrease, or cause no change in the rate of evaporation from the lake?

Question 4. Which will evaporate faster, a pan of hot water placed in the refrigerator or the same pan left at room temperature and why?

Question 5. Does evaporation affect water temperature, and if so how? Why or why not?

Question 6. If you wanted to compress some water vapor into a smaller space but keep the pressure constant, what would you do? Why?

Question 7. On a hot humid day, you must sweat *more* or *less* or *the same amount* as on a hot dry day at the same temperature. Why?

Question 8. If you had two glasses of water sealed in an air-tight container, and one was half filled with pure water, while the other half was filled with salt water, what would you expect to happen after a long period of time (say about a month)? Why?

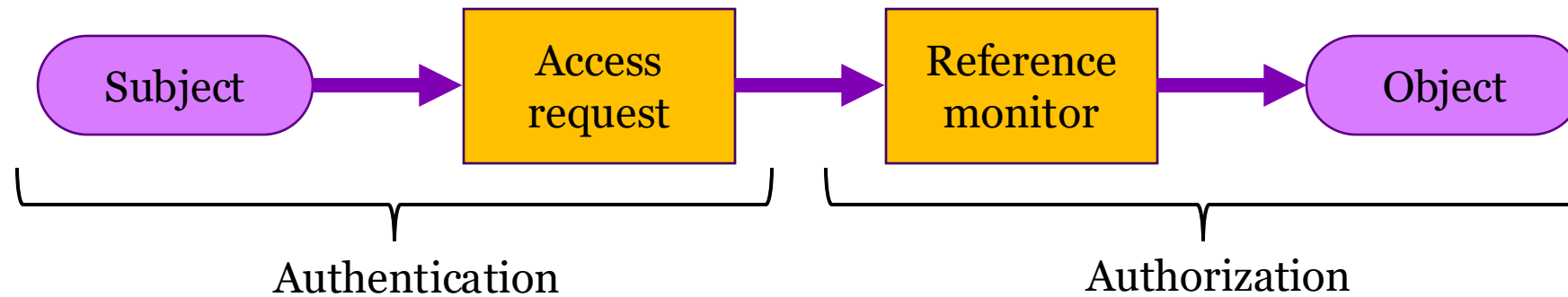
ACCESS CONTROL

Access Control

- Ensure that certain users can use a resource in one way (i.e. read-only), others in a different way (i.e. modify), and still others not at all.
- **Subjects** – human users who are often represented by surrogate programs running on behalf of the users
- **Objects** – things on which an action can be preformed. Such as files, database tables, programs, memory objects, hardware, network connections, and processors. User accounts can also be objects since they can be added to the system, removed, and modified.
- **Access modes** – any controllable actions of subjects on objects, including read, write, modify, delete, execute, create, destroy, copy export, and import.

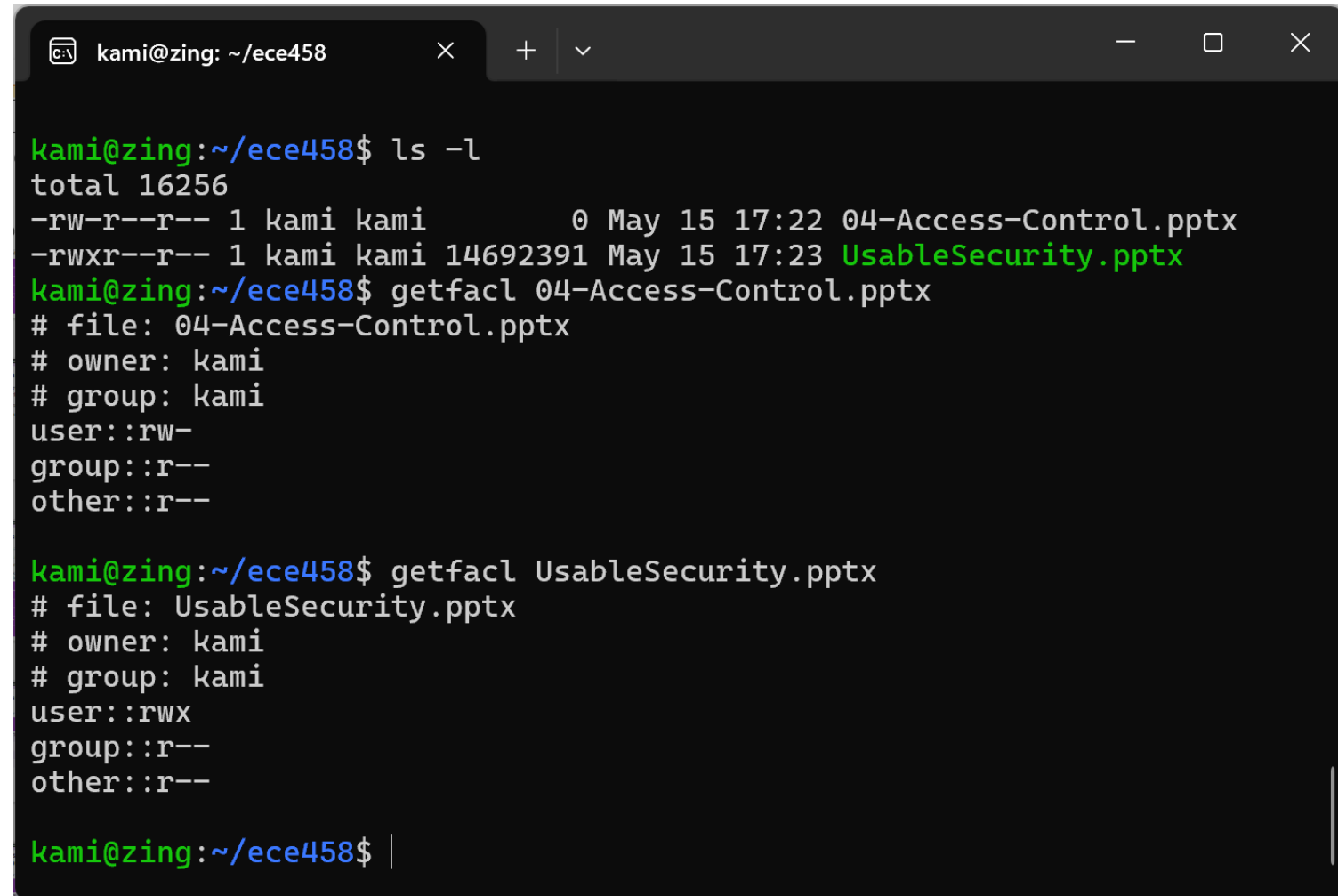
Access control

A guard controls whether a principal (the subject) is allowed access to a resource (the object).



Linux uses the Access Control Lists model

- Every file has a **U**ser, **G**roup, and **O**ther
- The **U**ser is the owner
- The **G**roup is a list of users for whom these permissions will apply
- **O**ther refers to all users logged into this computer



```
kami@zing: ~/ece458
kami@zing:~/ece458$ ls -l
total 16256
-rw-r--r-- 1 kami kami      0 May 15 17:22 04-Access-Control.pptx
-rwxr--r-- 1 kami kami 14692391 May 15 17:23 UsableSecurity.pptx
kami@zing:~/ece458$ getfacl 04-Access-Control.pptx
# file: 04-Access-Control.pptx
# owner: kami
# group: kami
user::rw-
group::r--
other::r--

kami@zing:~/ece458$ getfacl UsableSecurity.pptx
# file: UsableSecurity.pptx
# owner: kami
# group: kami
user::rwx
group::r--
other::r--

kami@zing:~/ece458$
```

Access Control Matrix

- Matrix of all the Subjects (rows) and all the Objects (columns) with the access modes listed in the cells
- Clear and lookup is efficient
- Most of the matrix is empty since most Subjects do not have access to most Objects

	Bibliog	Temp	F	Help.txt	C_Comp	Linker	Clock	Printer
User A	ORW	ORW	ORW	R	X	X	R	W
User B	R			R	X	X	R	W
User S	RW		R	R	X	X	R	W
Sys Mgr				RW	OX	OX	ORW	O
User Svcs				O	X	X	R	W

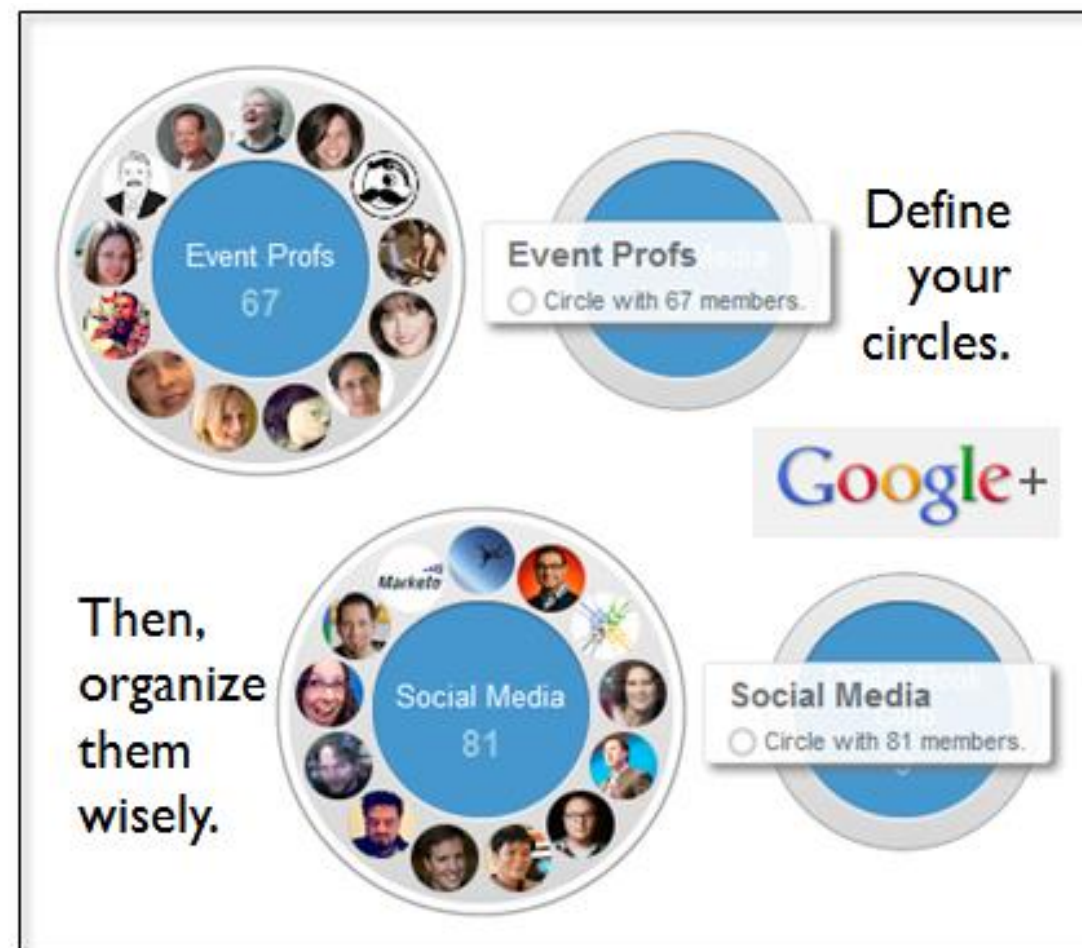
How does normal system access control differ from access control on social media and other online sharing platforms?

Traditional Access Control: Principle of least privilege

- A subject should have access to the smallest number of objects necessary to perform their task.
 - Example: A program does not need access to the absolute memory addresses to which a page number reference translates
 - Permissions should match what is possible. Impossible actions should not be granted
- Permissions should be reviewed and adjusted over time
 - New job, means new permissions and removal of old ones
 - Analyzing logs can show what permissions are not being used and can possibly be removed

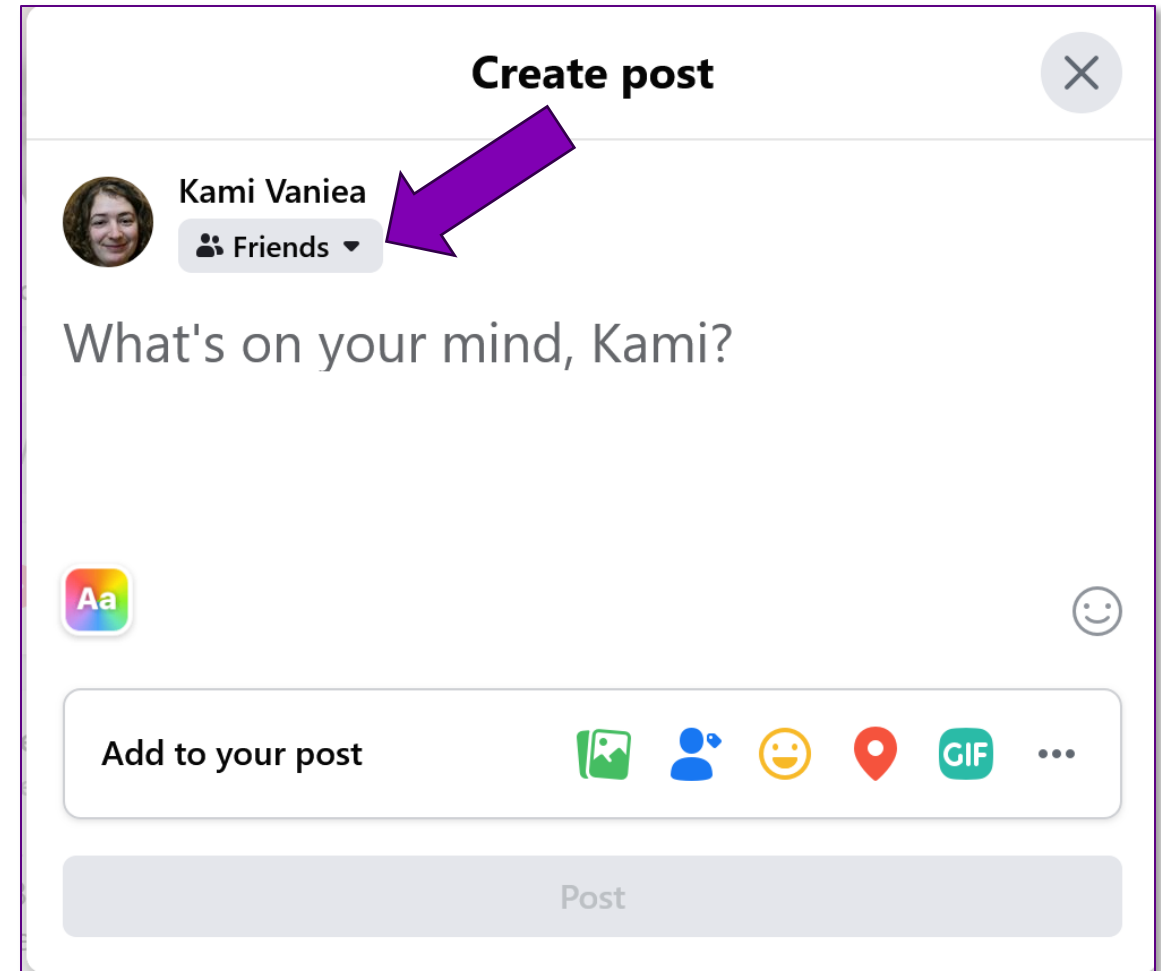
Social Media Access Control: Friends Lists

- Google+ tried to differentiate itself by creating “circles” so that you could organize your friends and posts




Social Media Access Control: Friends Lists

- Google+ tried to differentiate itself by creating “circles” so that you could organize your friends and posts
- Facebook has lists that control visibility at a post-level




Social Media Access Control: Friends Lists

- Google+ tried to differentiate itself by creating “circles” so that you could organize your friends and posts
- Facebook has lists that control visibility at a post-level
- Facebook Lists are even pre-populated (e.g. Friends) as well as configurable as groups or even custom


 **Post Audience**

Who can see your post?
Your post will show up in Feed, on your profile and in search results.


Your default audience is set to **Friends**, but you can change the audience of this specific post.

 **Public**
Anyone on or off Facebook

☐

 **Friends**
Your friends on Facebook

☒

 **Friends except...**
Don't show to some friends

☐

☒ Set as default audience.

[Cancel](#) [Done](#)

Social Media Access Control: Friends Lists

- Google+ tried to differentiate itself by creating “circles” so that you could organize your friends and posts
- Facebook has lists that control visibility at a post-level
- Facebook Lists are even pre-populated (e.g. Friends) as well as configurable as groups or even custom
- X (Twitter) has binary public/protected account-level control


What is the difference between public and protected posts?

- When you sign up for X, your posts are public by default; anyone can view and interact with your posts. Should you choose to protect your posts, you can do so through your [account settings](#). Learn more [protecting your posts](#).
- If you protect your posts, you'll receive a request when new people want to follow you, which you can approve or deny. Accounts that began following you before you protected your posts will still be able to view and interact with your protected posts unless you block them. Learn more about [blocking](#).

Who can see my posts?

- **Public posts** (the default setting): Are visible to anyone, whether or not they have a X account.
- **Protected posts**: Only visible to your X followers. Please keep in mind, your followers may still capture images of your posts and share them.


Facebook access control





Post Audience

Who can see your post?
Your post will show up in Feed, on your profile and in search results.

Your default audience is set to **Friends**, but you can change the audience of this specific post.


**Public**
Anyone on or off Facebook

**Friends**
Your friends on Facebook


**Friends except...**
Don't show to some friends


☒ Set as default audience.


[Cancel](#) [Done](#)





Post Audience

**Friends except...**
Don't show to some friends

**Only me**

**Specific friends**
Only show to some friends

**Custom**
Include and exclude friends and lists

**Associates**
Your custom list

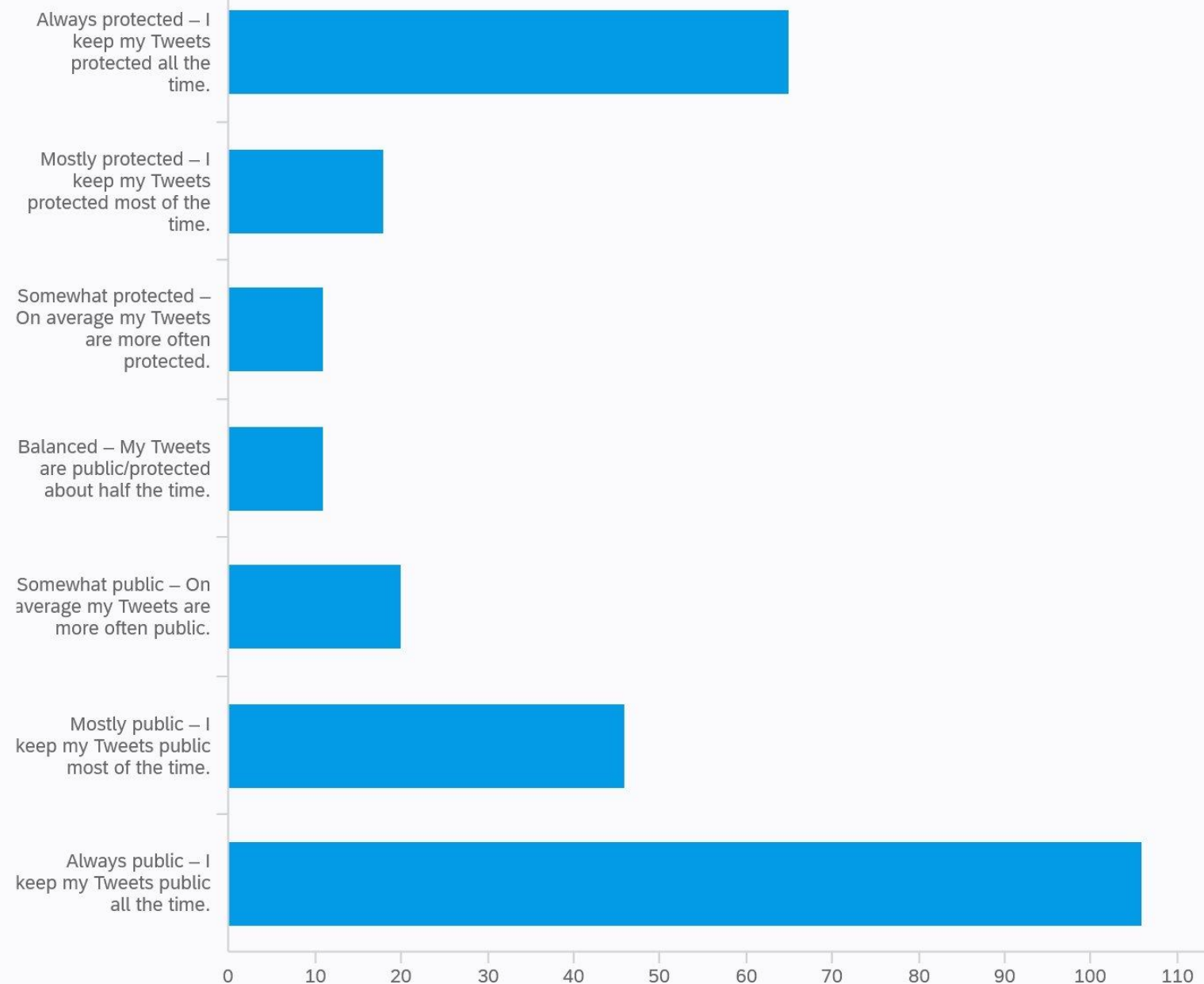
☒ Set as default audience.

[Cancel](#) [Done](#)

TWITTER (X) PRIVACY SETTINGS

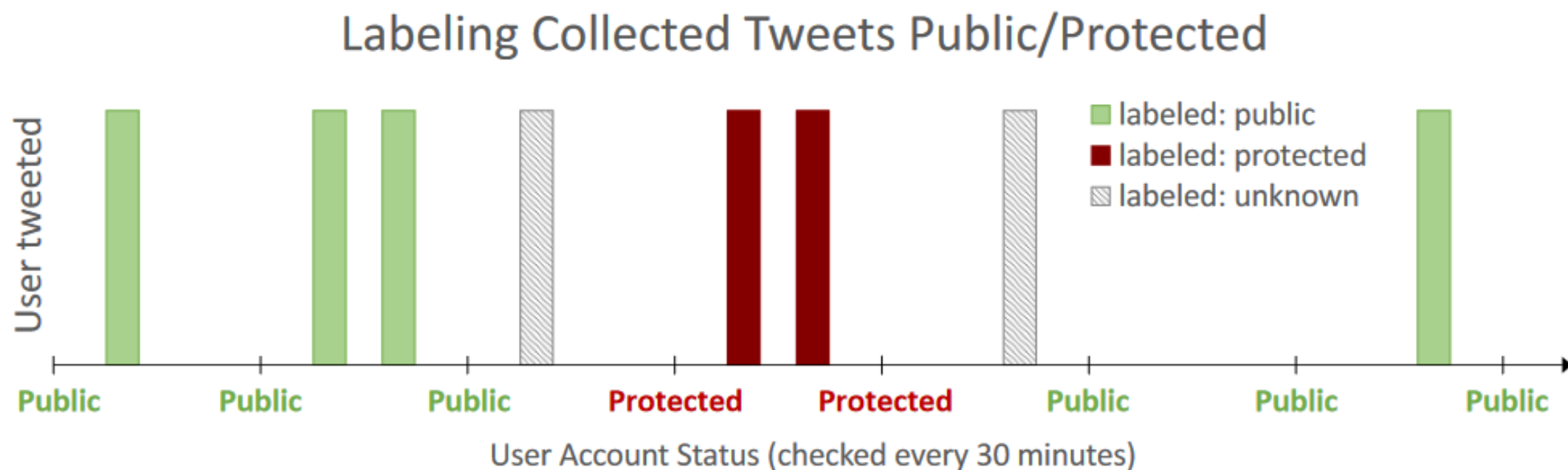
Which of the following best describes your normal Twitter audience?

- In prior Twitter research we collected tweets from users several times. We noticed that some users vanished and then re-appeared. Likely due to becoming protected.
- We conducted a survey asking the above question. Graph to the right is the result.



Collected tweets for 3 months

- Regularly polled accounts to see if they were protected or public
- Collected tweets when the accounts were public



Collected tweets for 3 months

- Regularly polled accounts to see if they were protected or public
- Collected tweets when the accounts were public

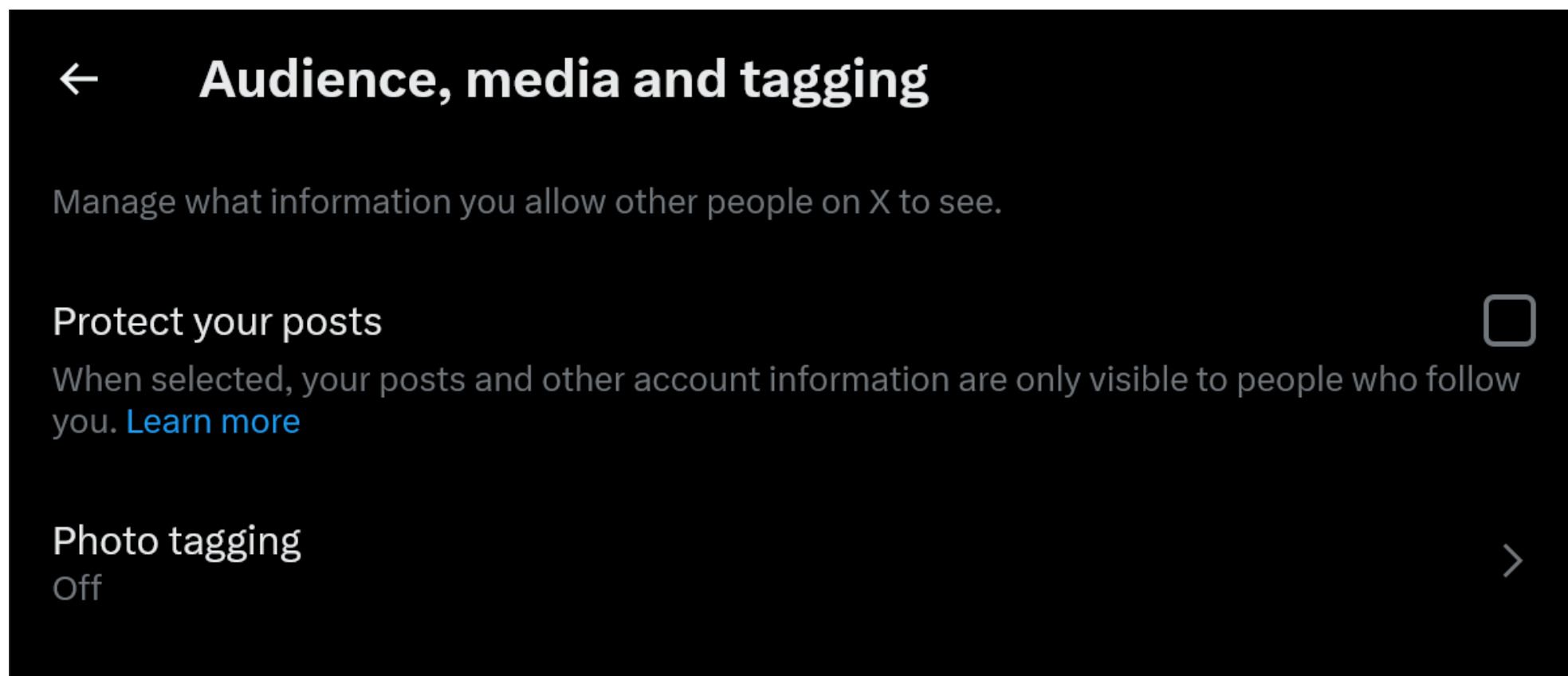
% time as protected	[0-10]%	(10-50)%	(50-90)%	90+%
# Users	2.6K	9.8K	10.3K	3K
Tweets while Public	5.3M	14.3M	6M	375K
Tweets while Protected	214K	3.4M	7.1M	2.5M
Total tweets	5.5M	17.7M	13.1M	2.9M

Do people intend to have the tweets they post while protected be publicly visible?

Do they understand how Twitter's access control system works?

X (Twitter) permissions

- Whole account is either protected or public



Reasons to turn public

Reasons to turn public	Twitter Data	Free-Text Survey
To reach a broader audience and get more interaction with my tweets		+
To gain more followers		+
To mention/reply to a user who does not follow me	+	+
To find potential employment		
To have a professional image		+
To sell things or receive donations		
To enter to get giveaways or freebies		+
To retweet other users	+	+
To quote tweet other users	+	+
To associate a tweet with hashtags or trends publicly	+	+
To boost the visibility, popularity, or ranking of a hashtag or topic		+
To boost the visibility of another user's tweet		
To share articles or links	+	
To share pictures	+	+
To get customer service		
To mention/reply to celebrities, famous people, or other VIPs	+	+

Table 8. Reasons to turn public - Options given in the survey and their sources

Reasons to turn protected

Reasons to turn protected	Twitter Data	Free-Text Survey
People I know found my account and that made me uncomfortable		+
My tweet unexpectedly went viral		+
I wanted to prevent non-followers from seeing tweets with personal content		+
To prevent people I know, such as friends and family, from seeing my tweets To archive the account without deleting it		+
To avoid harassment		+
To tweet about someone without them being able to see the tweets		+
To prevent account suspension		+
I did not want people to retweet me	+	
I did not want people to quote tweet me	+	
To talk about a sensitive, controversial, or political topics freely		+
To prevent interactions from strangers		+
To share pictures	+	+
To share content that is not safe for work (NSFW)		+
To retweet other users	+	
To quote tweet other users	+	+
To get a sense of privacy		+
To share articles or links	+	
To take a temporary break from interactions with non-followers		+

Table 9. Reasons to turn protected - Options given in the survey and their sources

Questions asked: two examples

Imagine Emily has a **public** account. Who can see Emily's tweets?

Anyone on the Internet can see Emily's tweets.

Anyone logged into Twitter can see Emily's tweets.

Only Emily's followers can see Emily's tweets.

No one but Emily can see Emily's tweets.

Imagine that Alex has her tweets set to **protected** and tweets about her new socks. She then changes her tweet visibility setting to **public**. After Alex changes the setting, who can see her tweet about her socks?

Anyone on the Internet can see Alex's sock tweet.

Anyone logged into Twitter can see Alex's sock tweet.

Only Alex's followers can see Alex's sock tweet.

No one but Alex can see Alex's sock tweet.

Users do not understand the public/protected setting

Individual Visibility Questions	Accuracy	
➡ Who can see a public account's tweets	86.9%	13% think only people logged into Twitter can see public tweets
Who can see a protected account's tweets	95.5%	
Change visibility from public to protected	89.3%	Public-> protected, 8% thought past Tweets would stay public
➡ Change visibility from protected to public	76.2%	
Keep visibility setting public	85.7%	Protected-> public, 7% thought past Tweets would stay protected

Table 2. Percentages of correct answers given to tweet visibility questions for an account.

Dilara Kekillioglu, Kami Vaniea, Maria K. Wolters, Walid Magdy (2023). [Twitter has a Binary Privacy Setting](#), are Users Aware of How It Works?. In Proceedings of the 2023 ACM SIGCHI Conference on Computer-Supported Cooperative Work and Social Computing (CSCW23).

Binary setting theoretically easy

- Twitter privacy is far more complex than public vs protected
 - People change their state over time for many reasons
- 7% of users think that if they change from protected -> public the old tweets will stay protected
- The “who would bother looking” attitude remains

QUESTIONS