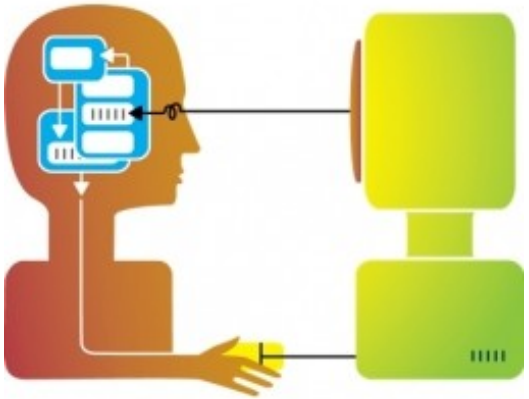
PRIVACY, SECURITY AND USABILITY

HCI and Usability

Topics

- What is HCI?
- What is usability?
- Usability and design
- Design process

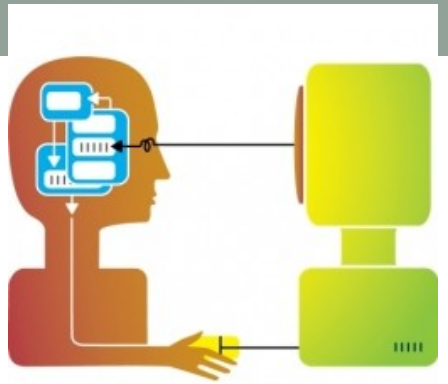
What is HCI?



- Human:
  - End user of programs
  - Subject of programs
  - Collaborators – coworkers, friends, colleagues
- Computers:
  - Machine programs run on
    - Often include client and server programs
  - Technology design and limitations
    - programming languages affect resulting program

https://www.iotone.com/term/human-computer-interaction-hci/t556

What is HCI?



- Interaction:
  - Users tell the machine what they want
    - Through the end-user programs

Humans

- Most computer users are NOT information security experts
  - but require assurance that they can trust the computer
- Often considered the “weakest link” within HCI

Humans

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations... But they are sufficiently pervasive that we must design our protocols around their limitations."

-- C. Kaufman, R. Perlman, and M. Speciner

Network Security: PRIVATE Communication in a PUBLIC World. 2nd edition. Prentice Hall, page 237, 2002

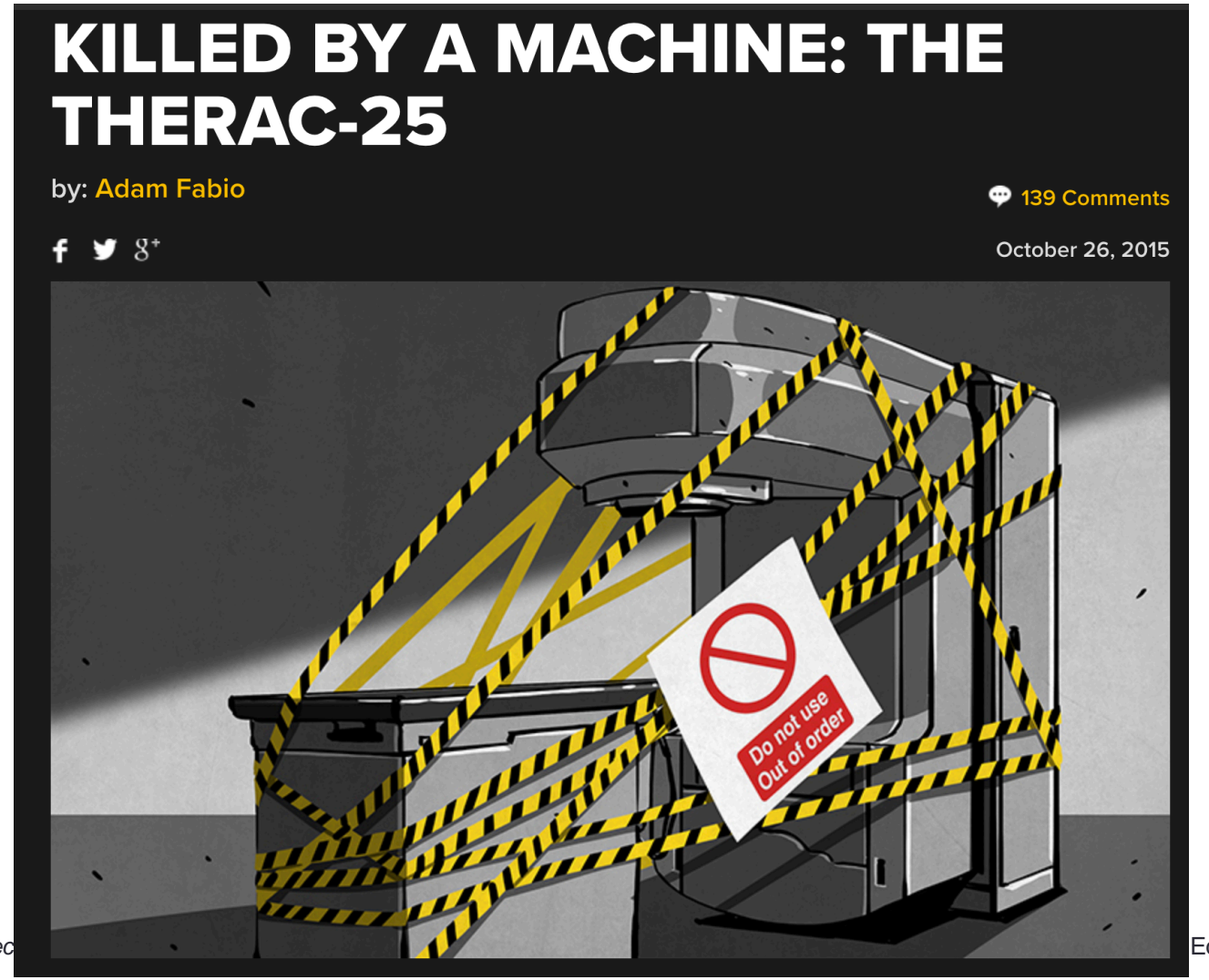
HCI is an Interdisciplinary Field

- Hardware Components from Computer Science, Engineering
- Process comes from design and product design
- Evaluation of design
  - Concepts from applied psychology, usability

Why is HCI Important?

- HCI is a major part of program design
  - Approximately 50%
- What are costs of bad user interface?
  - Money
    - User satisfaction drives profits
    - Good initial design easier than fixing problems later
    - Call center expenses
  - Reputation of organization (brand loyalty)
  - Time
    - User's time, produce redesign
  - May cause physical damage

Example – Costly HCI Mistake



THERAC-25

- A radiation therapy machine
- Involved in at least six accidents in 1985-1987
  - patients were given massive overdoses of radiation
- Messages like MALFUNCTION 1, MALFUNCTION 54, etc. were displayed when the machine detected conditions which placed patients at risk
  - but the errors meaning wasn't described in the operator's manual

THERAC-25

- Programming errors resulted in patient radiation doses that were hundreds of times greater than normal
  - resulting in death or serious injury

THERAC-25

- Side notes:
  - At the time, regulators were more aware of hardware failures but less aware of risks of software
  - ISO reviews afterwards started concentrating on software
  - HIPPA developed to help protect medical patient security and privacy

THERAC-25

- Therac-25 was manufactured by Atomic Energy of Canada Limited (AECL)
- AECL were not able to originally reproduce one of the problems
  - Running test after test
- Only after bringing a technician that was involved in 2 of the incidents to the lab and working with them was the issue reproducible

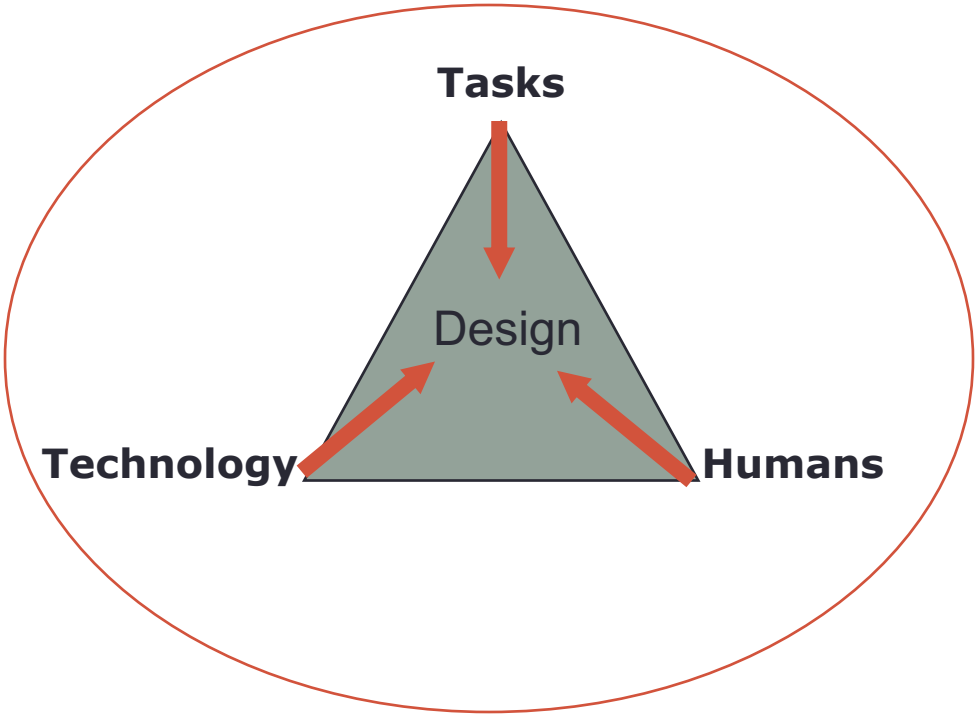
Example – Costly HCI Mistake:

- THERAC-25
  - Accidents highlighted the dangers of software control of safety-critical systems
    - Became a standard case study in health informatics and software engineering
  - Engineers' were overconfident in their initial work
    - failed to believe the end users' claims
    - Resulting in drastic repercussions

Why is HCI Important?

- User interfaces hard to get right
  - people are unpredictable
  - intuition of designers often wrong
  - need good design methods
- Privacy and Security
  - phishing scams
  - Information leakage (ex. location info, cookies)
  - Intrusion detection (diagnosis tools)
  - Intentionally circumventing security mechanisms

HCI Approach to UI Design



http://cups.cs.cmu.edu/courses/ups-sp06/slides/060119-overview-hci.ppt

HCI Approach to UI Design

- Examples of tasks:
  - high level:
    - writing a paper
    - drawing a picture
  - low level:
    - copying a word from one paragraph to another
    - coloring a line
- Other considerations:
  - Business models, level of fun

Good Design Myths

- Only experts create good designs
  - HCI techniques can be applied by anyone
    - faster, simple and effective
- We can fix the user interface at the end
  - good design is more than just user interface
    - having right features, building those features right

Good Design Myths

- Good design takes too long / costs too much
  - effective techniques can reduce total development time & cost
    - finds problems early on
- Good design is just cool graphics
  - graphics part of bigger picture
  - Need to define what needs to be communicated & how

What makes something usable?

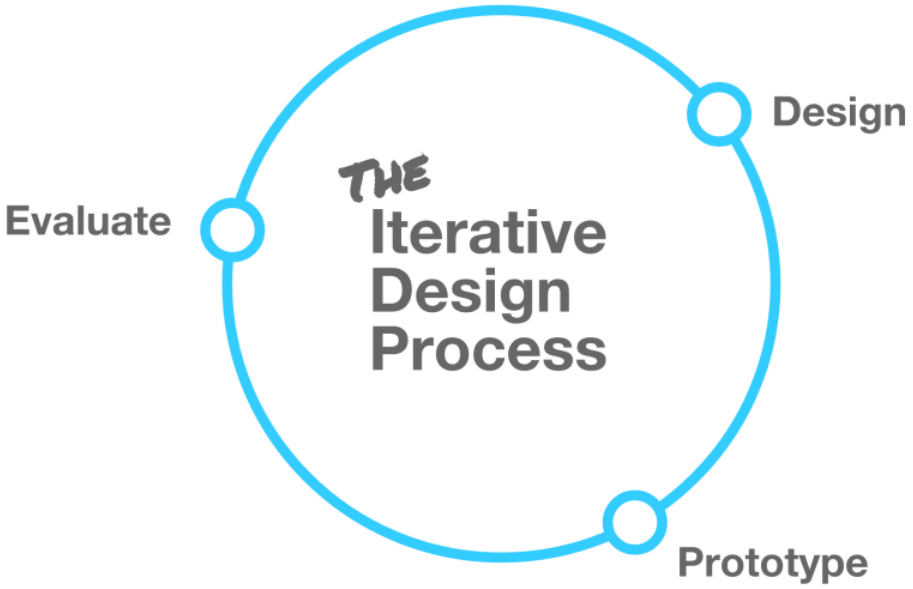
- Intuitive / obvious
- Efficient
- Learnable
- Memorable
- Few errors
- Not annoying
- Status transparent

User Interface is a Team Effort

- Participants may include:
  - graphic designers, interaction / interface designers
  - information architects, software engineers
  - technical writers, marketers
  - test engineers
  - usability engineers
  - Users
    - Through usability testing

HCI Design Cycle Is Iterative

- Design
- Prototyping
- Evaluation



https://www.shapeways.com/blog/archives/27235-jewelry-prototyping-tips.html

Design

- Design is driven by requirements
  - focus on the core need
    - not how it is to be implemented
- The process is iterative
  - Your process may start at any given point
    - And continue any number of times

Design

- A design is a simplified representation of the desired product
  - UI representations may include
    - product prototypes
    - description of tasks (text), showing tasks structure
    - screen sketches
    - flow diagrams / outline
  - Creating a product representation allows the designer to take a step back
    - consider how you can improve your design

Usability Goals

- “The effectiveness, efficiency, and satisfaction with which specified users achieve specified goals in particular environments”

ISO

Usability Goals

- Goals should be set at initial stages
  - Used later to measure progress
- Goals often have tradeoffs
  - Prioritize design parameters

Usability goals

- Effective
  - how well the program does what it is designed to do
    - users can easily find the information they seek, shoppers can easily complete purchases, clients can use the back-end control panel, etc.
- Efficient
  - perform tasks quickly
- Utility
  - Does the product do what it should do?
    - E.g., does a website offer the tools visitors will expect to find when they visit?
  - Utility is a measure of the product functionality.

Usability goals

- Learnable
  - Easy to learn
    - how fast first time visitors can complete tasks
- Memorable
  - How quickly a user can recall how to navigate and use the program
- Flexible
  - multiple ways to accomplish tasks

Usability Goals

- Robust
  - minimal error rates
  - good feedback
    - so user can recover from mistakes
- Pleasing, fun
  - high user satisfaction

DON NORMAN'S DESIGN PRINCIPLES

Interaction Design: Beyond Human-Computer Interaction, New York: Wiley, p.21

Design Principles

- Visibility:
  - The more visible functions are, the more likely users will be able to know what to do next
    - In contrast, when functions are "out of sight," it makes them more difficult to find and know how to use.
- Feedback:
  - Sending back information about what action has been done and what has been accomplished
    - allowing the person to continue with the activity
    - Various kinds of feedback are available for interaction design:
      - audio, tactile, verbal, etc.
- .

Design Principles

- Constraints:
  - Determining ways of restricting the kind of user interaction that can take place at a given moment
    - There are various ways this can be achieved.
- Mapping:
  - The relationship between controls and their effects in the world
    - Nearly all artifacts need some kind of mapping between controls and effects, whether it is a flashlight, car, power plant, or cockpit.
    - An example of a good mapping between control and effect is the up and down arrows used to represent the up and down movement of the cursor, respectively, on a computer keyboard.
- .

Design Principles

- Consistency:
  - Designing interfaces to have similar operations and use similar elements for achieving similar tasks.
    - In particular, a consistent interface is one that follows rules, such as using the same operation to select all objects.
    - For example, a consistent operation is using the same input action to highlight any graphical object at the interface, such as always clicking the left mouse button.
    - Inconsistent interfaces, on the other hand, allow exceptions to a rule.

Design Principles

- Affordance:
  - A term used to refer to an attribute of an object that allows people to know how to use it.
    - For example, a mouse button invites pushing (in so doing acting clicking) by the way it is physically constrained in its plastic shell.
    - Simply speaking, to afford means "to give a clue" (Norman, 1988)
    - When the affordances of a physical object are perceptually obvious it is easy to know how to interact with it.

Design and Happiness

- The three ways that good design makes you happy - Don Norman

Quantifying Usability

- What can we measure?
  - Speed
  - Efficiency
  - Learnability
  - Memorability
  - User Preference

Quantifying Usability

- Speed
  - How quickly can a specific task be accomplished?
    - Time the user takes to achieve it
    - Disregarding user mistakes
  - Can be measured in time units (seconds, etc.)
- Efficiency
  - How many mistakes were made trying to achieve the task?
    - Example: trying to type faster would result in increased speed but likely also in reduced efficiency
      - More typing mistakes
  - Can be measured by counting mistakes

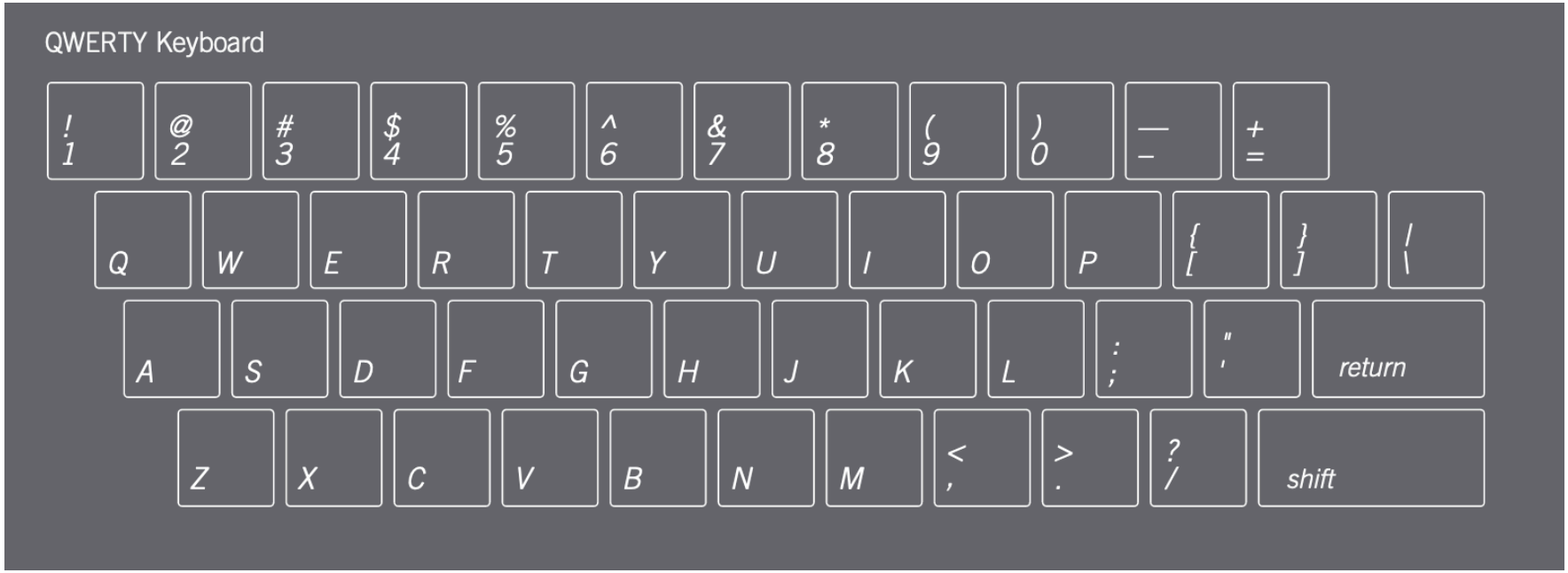
Quantifying Usability

- Learnability:
  - How easy it is for a user to learn the system?
    - For the first time he is using it
- Memorability:
  - How easy is it to remember how to use the system?
    - Once the user already learned it
- Both measured in time units (seconds, etc.)

Quantifying Usability

- User Preference
  - Which system/features does the user prefer?
    - User may prefer slower system or less efficient one
  - Can be measured through survey questionnaire
    - Standard questionnaires exist

User Preference vs. Performance -



http://people.sunyit.edu/~lepres/thesis/principles/181_pdfsam_POD.pdf

User Preference vs. Performance -

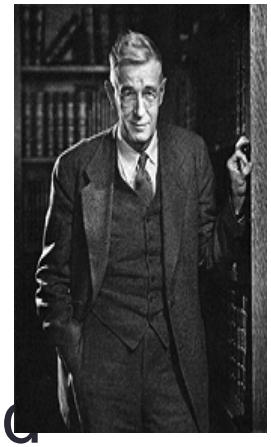
http://people.sunyit.edu/~lepres/thesis/principles/181_pdfsam_POD.pdf

User Preference vs. Performance

- Example: The QUERTY vs. the DRORAK keyboards
  - QUERTY keyboard originally designed to prevent jamming
    - On mechanical typewriters
  - DVORAK keyboard designed to maximize efficiency
    - Resulted in 30% typing efficiency
  - Because of historical reasons, QUERTY keyboard still the preferred keyboard
    - Users already familiar with it, exists on many current devices

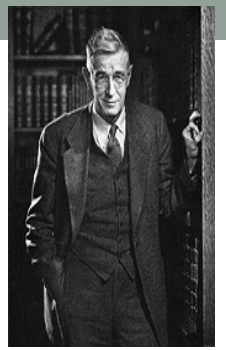
HCI HISTORY

Vannevar Bush - HCI Visionary



- Faculty member in MIT
- Established a partnership between the United States military and university research
  - coordinated WWII effort with 6000 US scientists
  - subsequently led to the development of the ARPANET
- Social contract for science
  - federal government funds universities
  - universities do basic research
  - research helps economy & national defense

Vannevar Bush (cont.)



- Wrote "As We May Think" in 1945
  - A visionary description of the potential use for information technology
    - Memex
      - Memex was never created
    - Other technologies:
      - wearable cameras for photographic records, encyclopedia Britannica for a nickel, automatic transcripts of speech, etc.
  - Inspiring creators of the internet
    - Licklider, Engelbart, etc.

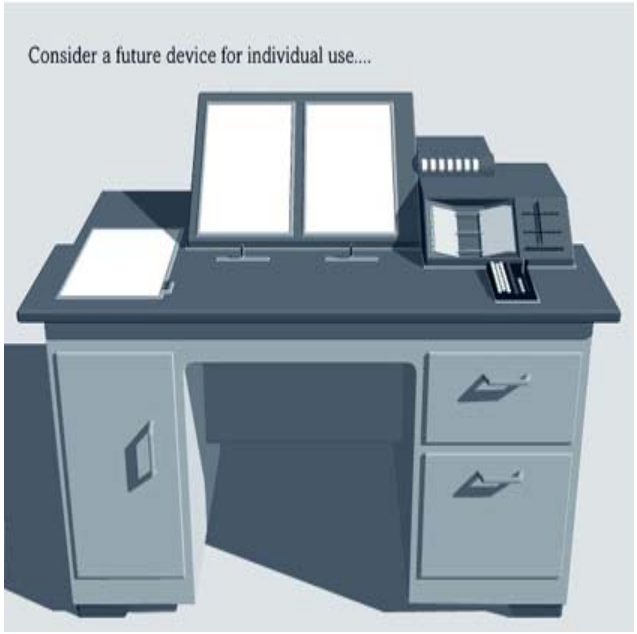
"As We May Think" [Vaneer Bush]

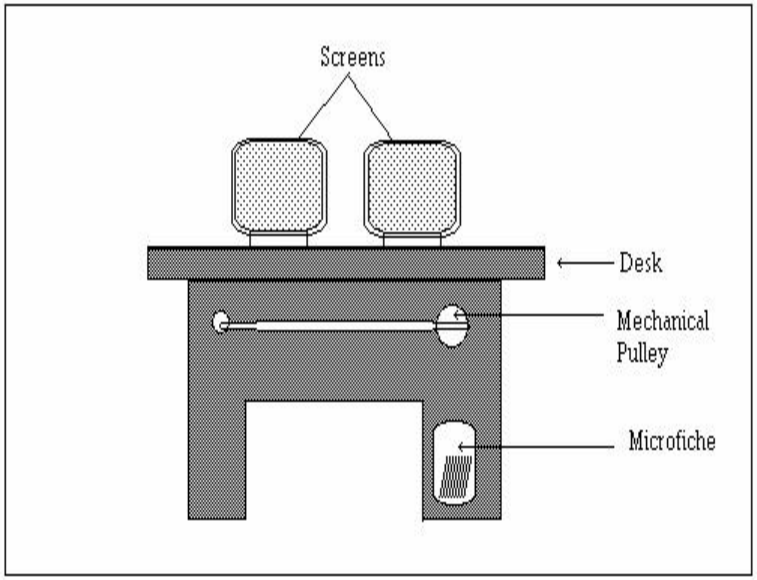
- Very optimistic about future
  - technology could help society
  - technology could manage flood of info
- He was one of the most informed people of his time
  - look at trends, guess where we're going
- What was he right about? Wrong about?

Memex (As we may think)

- A device in which individuals would compress and store all of their books, records, and communications
- Would provide enlarged supplement to one's memory
- The concept of the memex influenced the development of early hypertext systems
  - Text with hyperlinks leading to other text
  - Eventually led to the creation of the World Wide Web

Memex





https://cs.brown.edu/stc/resea/telecollaboration/story.html

https://userpages.umbc.edu/~rada/cv/pubs/hypertextbook/chapter3.html

Memex

- Mechanized private file and library
- May be consulted with exceeding speed and flexibility
  - To search books, records, and communications
- It consists of a desk
  - May be operated from a distance, but it is primarily a piece of furniture
  - User works next to it

"As We May Think"

- Have come true:
  - flood of information
  - faster / cheaper / smaller / more reliable
- Not implemented (yet):
  - microphotography
  - memex

Computers and HCI

- Computers in the past:

https://www.telegraph.co.uk/technology/7955813/The-history-of-computers.html
https://www.telegraph.co.uk/technology/7955813/The-history-of-computers.html

Computers and HCI

- Today:
-
-

Computers and HCI

http://www.uscensus2010data.com/the-evolution-of-technology-the-history-of-computers/

What Changed?

- Computer languages evolved
  - FORTRAN, a high level programming languages introduced in 1954
    - Before that, only assembly and or binary programming used
  - Enabled more people to start program easily
- New interface mechanisms created
  - Mouse introduced in 1964 by Douglass Engelbart
- Computer games created
  - First game, Spacewar, created in 1962 by Steve Russel and MIT
- ARPANET created in 1969
  - Evolved into the internet we know today

Douglass Engelbart

- Founder of Human-Computer Interaction field
  - While at Augmentation Research Center at RSI Lab
- Inventor of the mouse
- Looked for a way to solve problems
  - Through augmenting human intelligence and developing ways of building collective intelligence

https://en.wikipedia.org/wiki/Douglas_Engelbart

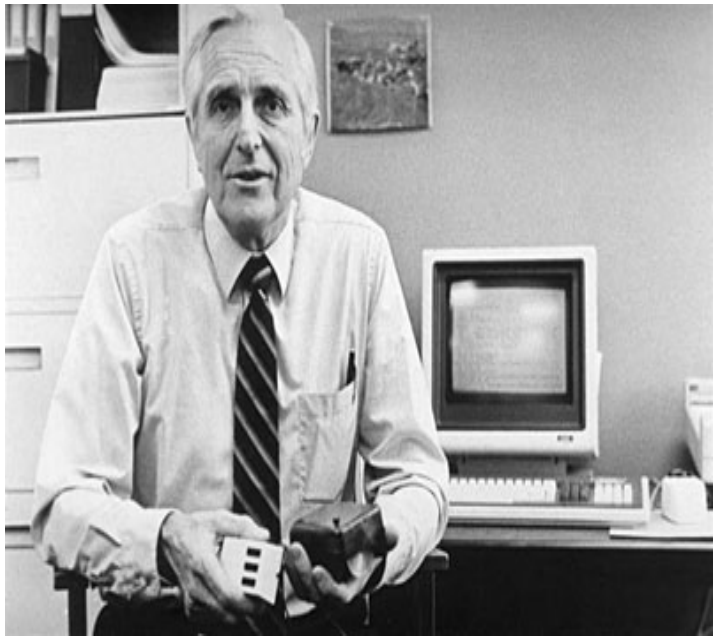
Augmenting Human Intellect

- First mouse introduced in 1964
- Engelbart discussed steps in development:
  - “At SRI in the 1960s we did some experimenting with a foot mouse. I found that it was workable, but my control wasn't very fine and my leg tended to cramp from the unusual posture and task. I assume that these would be overcome eventually by practice. “
    - Foot pedals previously used in sewing machines, etc.

Augmenting Human Intellect

- First mouse introduced in 1964
- Engelbart discussed steps in development (cont.):
  - “I got to thinking about skill development with fine foot control, and realized that most of us developed a very high degree of fine control with the accelerator pedal. I tried controlling vertical cursor position with such a pedal, and it worked quite well. Thinking about concurrent horizontal control, I realized that I can swing my knee from side to side with fairly good control (in terms of fraction of the total range of swing). That worked fairly well, better, I found, than with the foot mouse.”

Invention of the Mouse



http://history-computer.com/ModernComputer/Basis/mouse.html

Invention of the Mouse

Bill English, Engelbart's leading engineer, tests first moues and keyboard

http://history-computer.com/ModernComputer/Basis/mouse.html

Douglass Engelbart

- https://www.youtube.com/watch?v=vdFejSdS9fs

Douglass Engelbart - Demo

- https://www.youtube.com/watch?v=yJDv-zdhzMY

Augmenting Human Intellect

- What was the contribution of Engelbart to HCI?
  - in terms of devices, interactions, & apps
  -

Augmenting Human Intellect

- First mouse
- First hypertext
- First word processing
- First 2D editing & windows
- First document version control

Augmenting Human Intellect

- First groupware (shared screen teleconferencing)
- First context-sensitive help
- First distributed client-server
- Many other ideas!

Augmenting vs. Automation – Douglas Engelburt

"I tell people: look, you can spend all you want on building smart agents and smart tools…"

"I'd bet that if you then give those to twenty people with no special training, and if you let me take twenty people and really condition and train them especially to learn how to harness the tools…"

"The people with the training will always outdo the people for whom the computers were supposed to do the work."

HUMAN FACTOR

Human Studies

- Human-Computer Interaction (HCI) studies how humans interact with computers and other technology
  - Often with goal of improving this interaction through better design

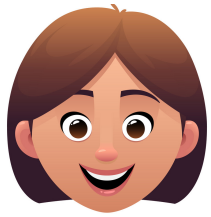
Human Studies

- Human-Computer Interaction (HCI) studies how humans interact with computers and other technology
- This requires understanding humans
  - And not just you!
    - Everyone is different
      - Different background, experience, behavior, etc.
  - Observe humans
  - Develop personas of different users
    - Based on their characteristics

Human Personas

- Method developed in the 1990's
- Used in development of products, marketing, planning of communication
- Does not look at the entire person
  - Highlight the aspects relevant to your work, design, etc.

An example Persona



- Name: Michelle
- Age: 30
- Occupation: sales manager in Target
- Hobbies:
  - outdoor hiking, swimming,
  - Takes trips with her husband and children on the weekend
- Michelle is very busy and treats time as a commodity
  - Prefers efficient applications
- Favorite activities:
  - SMS's to family and friends
  - Phone calls to friends
    - Calls may take 30 minutes
  - Likes using twitter
- Dislikes:
  - Cold sales call
  - Complicated applications

https://www.vectorstock.com/royalty-free-vector/young-woman-head-avatar-cartoon-face-character-vector-21787880

Personas

- A persona is not a person
- You do not look at the entire person
  - use the area of focus or domain you are working within as a lens
    - to highlight the relevant attitudes and the specific context associated with the area of work

Personas

- Personas

Security and the human factor

- How do humans affect security?
  - Human may be malicious
  - Humans may make mistakes
    - Lack of training
    - Rushing users
    - Busy and trying to multi-task
  - Constrained by limitations
  - Unmotivated users
    - Part of job obligations, not passionate about product

Key Challenges

- Security is a secondary task
  - Users are trying to get something else done
- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Human capabilities are limited
  - Memory, patience, different knowledge levels and background
- Active adversaries
  - Unlike traditional HCI design

Humans and Security

- Users typically concerned about usability
  - Fun, reward of applications
  - Availability is important
    - “don’t lock me out”
  - Security is a secondary consideration
- Security concerned with keeping the system safe
  - “keep the bad guys out”
- Different concerns for users and security experts!

Improving usability of secure systems

- Make security invisible
  - Device functionality stays the same
  - Security methods work in background
- Make security/privacy understandable
  - Make it visible, intuitive
  - Use methods that user can relate to
- User training

What makes a system unusable?

- Unhelpful user interface
  - Misleading/confusing
- Asking the user to make certain decisions
  - User may not be be knowledgeable or qualified to make them
  - Keep user interface simple

What makes a system unusable?

- Assuming user can provide his undivided attention to program
  - User may be rushing/busy, may be able to only exert limited effort

Understand the human factor

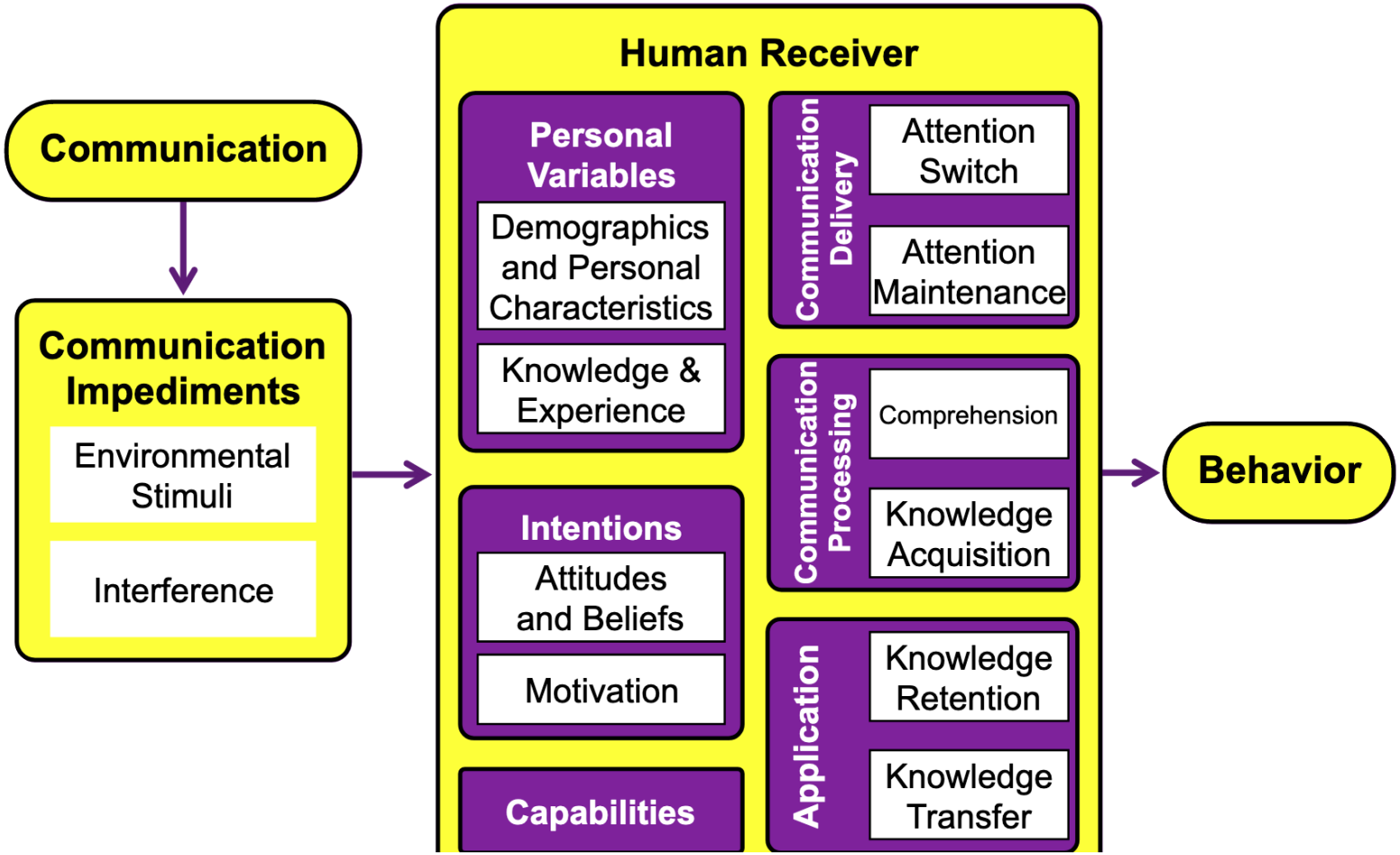
- Need to ensure that:
  - Users know they need to do something
  - Users know what it is they need to do
  - Users know how to perform the task
  - Users are interested/motivated to do it
  - Users have the knowledge/capability to do it

Human-in-the-loop Security Framework*

- Developed by Models human interaction with secure systems
- Can help identify (non-malicious) human threats

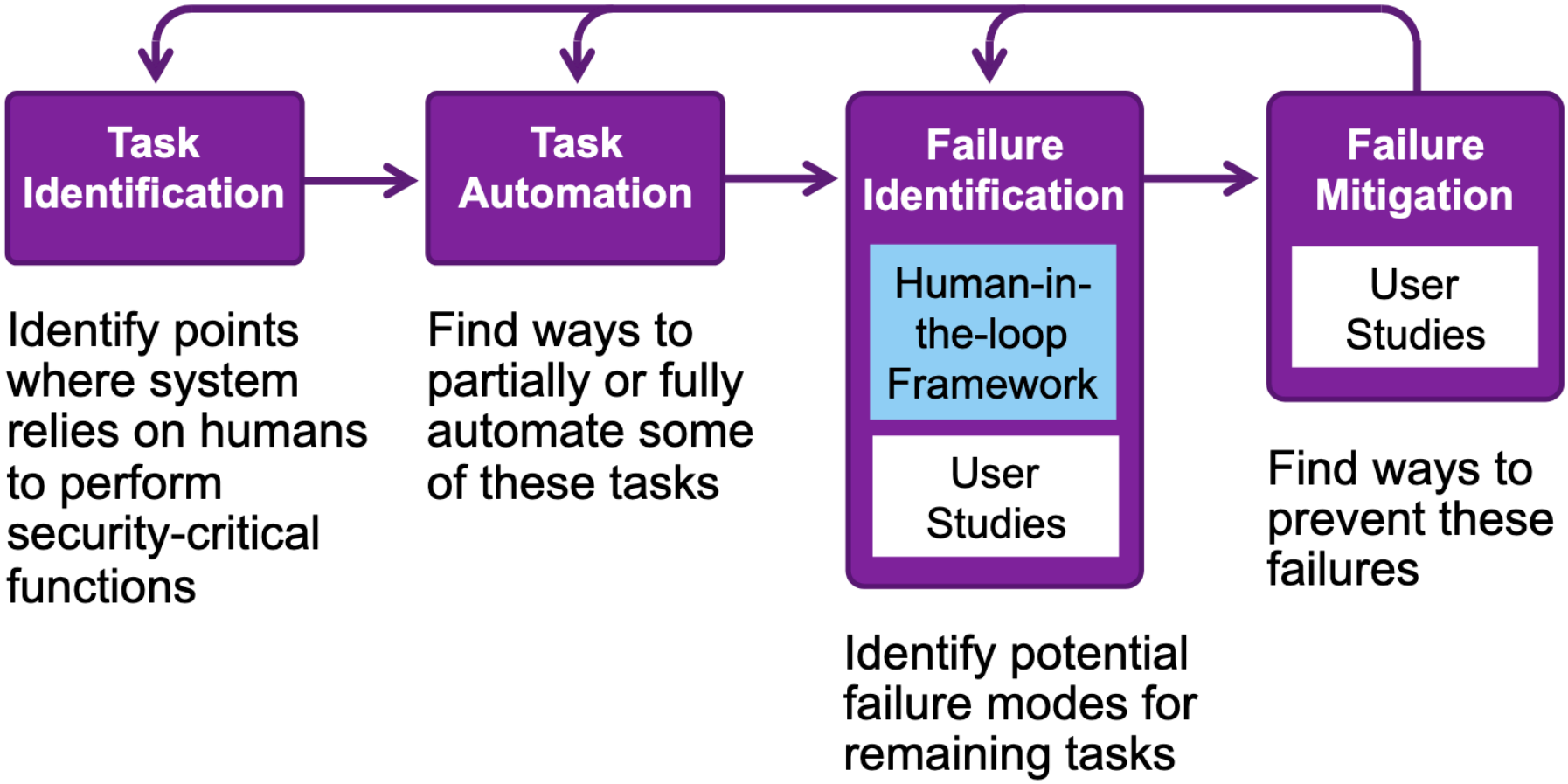
- *L. Cranor. A Framework for Reasoning About the Human In the Loop. Usability, Psychology and Security 2008

Human-in-the-loop Security Framework



http://users.umiacs.umd.edu/~mmazurek/818D-S15/slides/02-human-loop.pptx.pdf

Human threat identification and mitigation



http://users.umiacs.umd.edu/~mmazurek/818D-S15/slides/02-human-loop.pptx.pdf

User-Centered Approach

- Early focus on users and tasks
  - Know your user
    - Cognitive abilities
      - perception
      - physical manipulation
      - memory
    - Organizational / job abilities

User-Centered Approach

- Early focus on users and tasks (cont.)
  - Intended users should use simulations/prototypes to carry out real tasks
    - Early in the process
      - Through usability studies, etc.
    - Their performance and reactions should be observed, recorded and analyzed

You are not the user

- Seems obvious, but…
  - different experiences
  - different terminology
  - different ways of looking at the world
- Easy to think of self as typical user
- Easy to make mistaken assumptions
  - Just because you can use it doesn't mean other users will be able to
    - You may be more knowledgeable!

User-Centered Approach

- Keep users involved throughout the design
  - understanding work process
  - getting constant feedback
- User-centered design mind-set
  - thinking of the world in users' terms (empathy)
  - not technology-centered / feature driven, think of benefit to users

Basic Activities of Interaction Design

- User requirement analysis
  - Building users profiles
  - User task analysis
  - Data and platform constraints
    - Privacy, data sharing needs
    - Devices, software, hardware
    - Networks
  - Incorporating usability design principles

Basic Activities of Interaction Design (cont.)

- Building/prototyping alternative designs
- Evaluating designs

User Requirement Analysis

- Learn the users and the tasks they need to perform
  - How do user partition the tasks and sequence them
- Observe existing work practices
- Create scenarios of actual use
- This lets us try new ideas before building the product!
  - Get rid of problems early in the design process
    - while they are still cheap to fix!

Who is the user?

- Types of users
  - For a broad product, may need to define several different user types
    - More complex
  - Easier to design for a specific customer or in-house product
- Background
  - What are the values of the user? How do we integrate them into the product?

Who is the user?

- Skills
  - Knowledge, ability to learn, etc.
- Work habits and preferences
  - Time constraints, space, etc.
- Physical characteristics
  - Is vision, right/left handed, height, etc. a factor?

Task Analysis

- Understand relative importance of tasks
  - Important tasks should take priority
    - More accessible, more efficient

Task Analysis

- Where is the task performed?
  - Office, laboratory, point of sale?
    - What are the effects of environment on users?
  - Are users under stress?
  - Are there confidentiality required?
  - Other potential constraints:
    - Wet, dirty, or slippery hands?
    - Lighting? Noisy?

Hierarchical Task Analysis

- Disintegrating tasks into subtasks
  - Splitting tasks into sub-tasks and in sequence
  - Subtasks could be analyzed using the logical sequence for execution
  - helps in achieving the goal in the best possible way
- Identify instructions that users need to know

Task Analysis

- How often will users perform the task?
  - Frequent users remember details better
  - Infrequent users need more help
- Which functions are performed more frequently?
  - System should be optimized for these tasks
    - Better usability
- What Other Tools Does the User Have?
  - How does the user work with collection of tools to perform tasks

Error Handling

- How do people handle task related errors?
- What are the risks?
  - If systems becomes unavailable, being hacked, etc.
- Is there a backup strategy?

Data Confidentiality and Access

- Is the data public?
  - Online social networks, public web sites, open government records,
- Personal data?
  - Ex. health records, bank records
  - Is the data encrypted?
  - Is it always accessed at same machine or do users move between machines?
    - Manage network confidentiality

Data Confidentiality and Access

- Should data access be restricted?
  - Develop access models
- Remote access required?
  - VPN's?

Involve users in design

- Users help designers learn:
  - what is involved in their jobs
  - what tools they use
  - i.e., what they do and how they do it
- Developers reveal technical capabilities
  - builds rapport & an idea of what is possible
  - user's can comment on whether ideas make sense

Involve users in design

- Go out to real users and get real data from them
  - find out what they really do
  - how would your system fit in
- Are they too busy?
  - buy their time (t-shirts, coffee mugs)
  - find substitutes (medical students)
- How do we do this?
  - observe & interview prospective users
    - If possible, in their work place
  - Run user studies

UX DESIGN

- UX Design

Questions?