PRIVACY, SECURITY AND USABILITY

Introduction

Class Information

- Tzipora Halevi
  Assistant Professor
  CUNY Graduate Center room 4327
- Class hours: Monday, 11:45am - 1:45 pm
- Office hours: Monday, 2:00 pm – 3:00 pm

Today's class

- Cybersecurity and HCI – introduction and motivation
- Syllabus and course policies
- Overview of course topics
- Student introductions

Syllabus

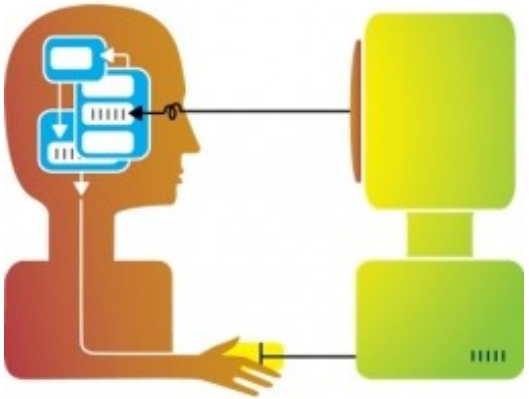
- Class Syllabus

Student Introduction

- Please take a moment to introduce yourself, including:
  - Your name, major, year of study
  - Why are you taking this class?
  - Can you name a security or privacy tool that you find annoying or can suggest improvements for?

CYBERSECURITY AND HCI

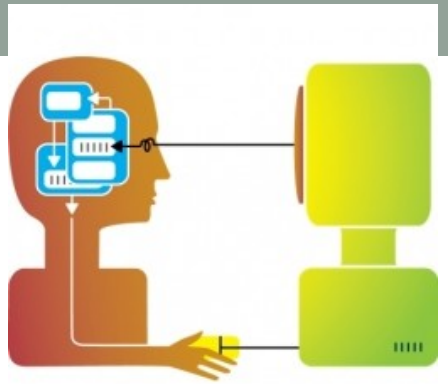
What is HCI?



- 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.”

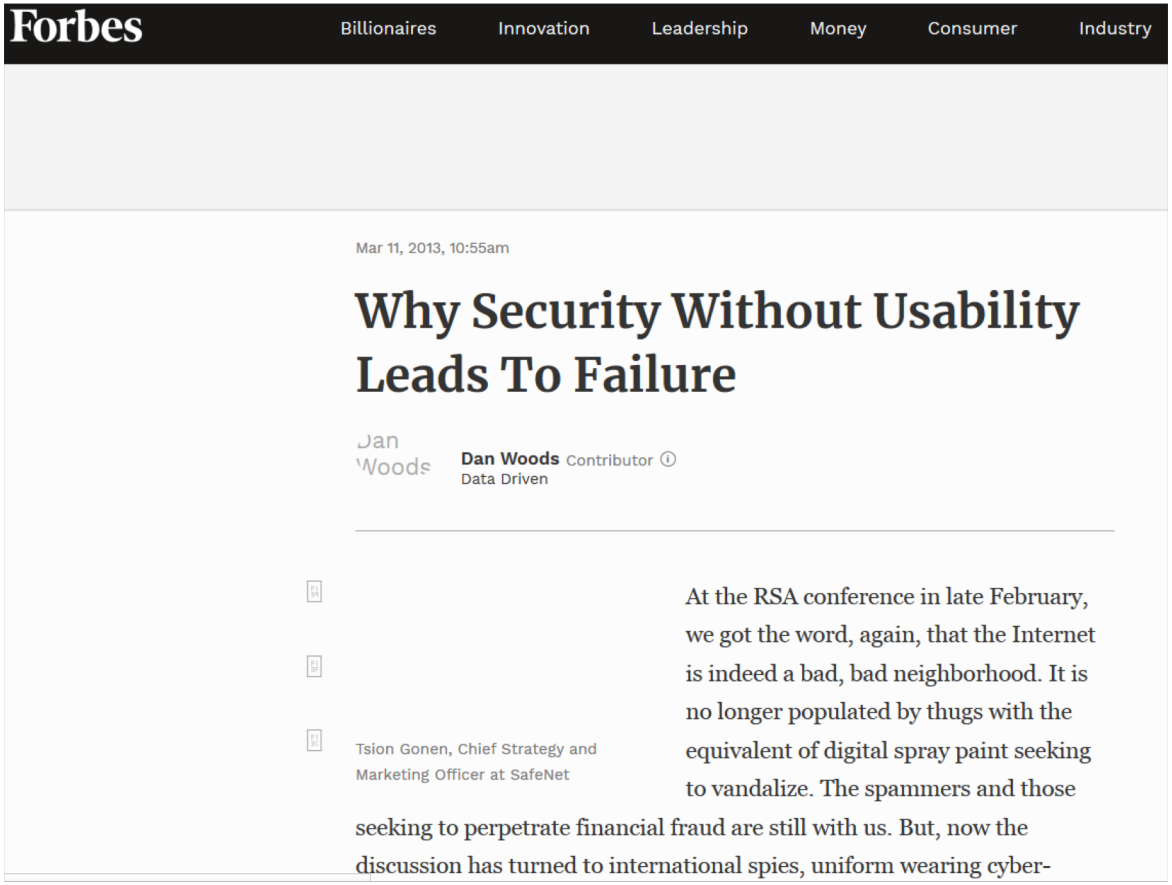
- −− C. Kaufman, R. Perlman, and M. Speciner.
- Network Security: PRIVATE Communication in a PUBLIC World.
- 2nd edition. Prentice Hall, page 237, 2002

https://www.forbes.com/sites/steveculp/2016/05/10/cyber-risk-people-are-often-the-weakest-link-in-the-security-chain/#4737ac3a2167

Cybersecurity and HCI

- Examining security/privacy and the human factor is often critical
  - For achieving both usability and security/privacy

Security and Usability



Forbes

Billionaires Innovation Leadership Money Consumer Industry

Mar 11, 2013, 10:55am

Why Security Without Usability Leads To Failure

Dan Woods

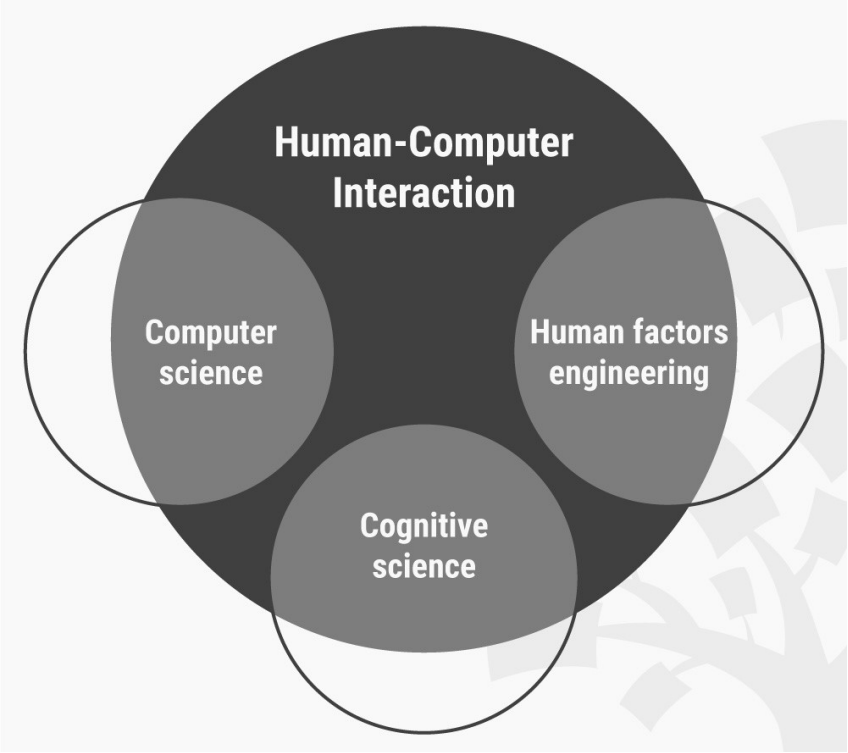
Dan Woods Contributor ⓘ
Data Driven

Tsion Gonen, Chief Strategy and Marketing Officer at SafeNet

At the RSA conference in late February, we got the word, again, that the Internet is indeed a bad, bad neighborhood. It is no longer populated by thugs with the equivalent of digital spray paint seeking to vandalize. The spammers and those seeking to perpetrate financial fraud are still with us. But, now the discussion has turned to international spies, uniform wearing cyber-

https://www.forbes.com/sites/danwoods/2013/03/11/why-security-without-usability-leads-to-failure/#8ca0ffa45336

Cybersecurity and HCI - Interdisciplinary Approach



https://www.interaction-design.org/literature/topics/human-computer-interaction

Cybersecurity and HCI - Interdisciplinary Approach

- Solutions and approaches from multiple disciplines can be applicable, including:
  - Computer science, engineering
  - Applied psychology
  - Behavioral economics
  - Cognitive sciences
  - CommunicationMarketing and design

Cybersecurity and HCI - Interdisciplinary Approach

- Solutions and approaches from multiple disciplines can be applicable, including (cont.):
  - Sociology
  - Counterterrorism
  - Risk perception
  - Network analytics

Cybersecurity and HCI

- Security approach: Humans are a secondary constraint to security constraints
- Usability/HCI: Humans are the primary constraint, security rarely considered
- Usable security: Human factors and security are both primary constraints

Security

- Human role in security:
  - Primarily adversaries/attackers
  - User studies rarely done
- Focused on quantitative metrics
- Uses threat models

Usability/HCI

- Concentrates on humans
  - Security rarely considered
  - User studies common
  - Involves cognitive, mental and task models

What is usability?

"The **effectiveness, efficiency and satisfaction** with which specified users achieve specified goals in particular environments."

ISO 924

https://www.w3.org/2002/Talks/0104-usabilityprocess/slide3-0.html

What is usability?

- **“effectiveness:** the accuracy and completeness with which specified users can achieve specified goals in particular environments
- **efficiency:** the resources expended in relation to the accuracy and completeness of goals achieved
- **satisfaction:** the comfort and acceptability of the work system to its users and other people affected by its use”

ISO 9241

https://www.w3.org/2002/Talks/0104-usabilityprocess/slide3-0.html

Motivation

- In security, we need to manage risks
- Typically define a threat model
  - Who is the adversary, his capabilities, resources
- Need to achieve two sometimes contradicting goals

Motivation

- Need to maintain systems security and privacy
  - Not depend on user
    - User may not be capable of managing security
    - Rushing user may make bad decisions
    - Attackers use human engineering methods to fool users
      - Lure them into make bad decisions
    - Users may not think about security and privacy
      - Only become aware of it if an attack occurs, side effects encounter

Usable Security

- Combines both security and human factors
- Humans are both users and potential adversaries
- User studies common
  - May involve deception, active adversary

Approaches to usable security

- Make it “just work”
  - Invisible security
- Make security/privacy understandable
  - Make it visible
  - Make it intuitive
  - Use metaphors that users can relate to
- Train the user

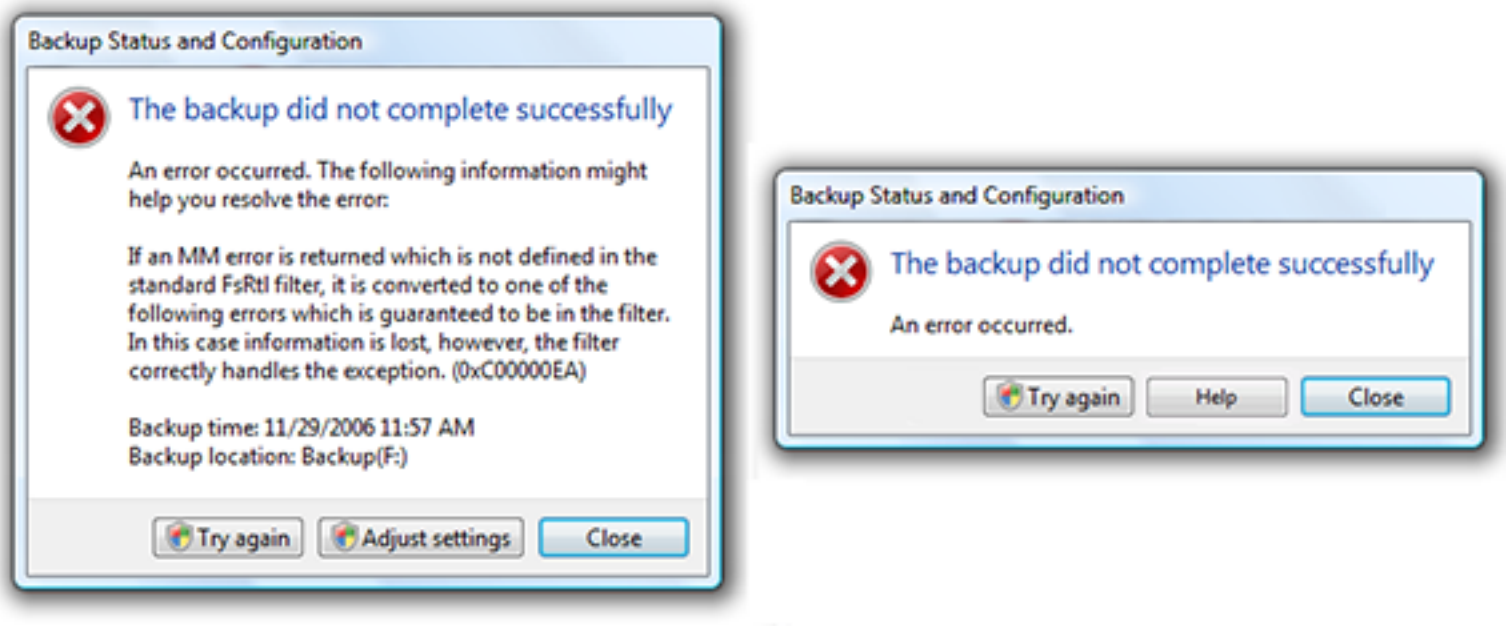
Design Choices – User Decisions

- Developers should not expect users to make decisions they themselves can’t make

Design Choices – User Decisions

https://www.techsupportforum.com/forums/f56/how-to-turn-off-certificate-warning-518108.html

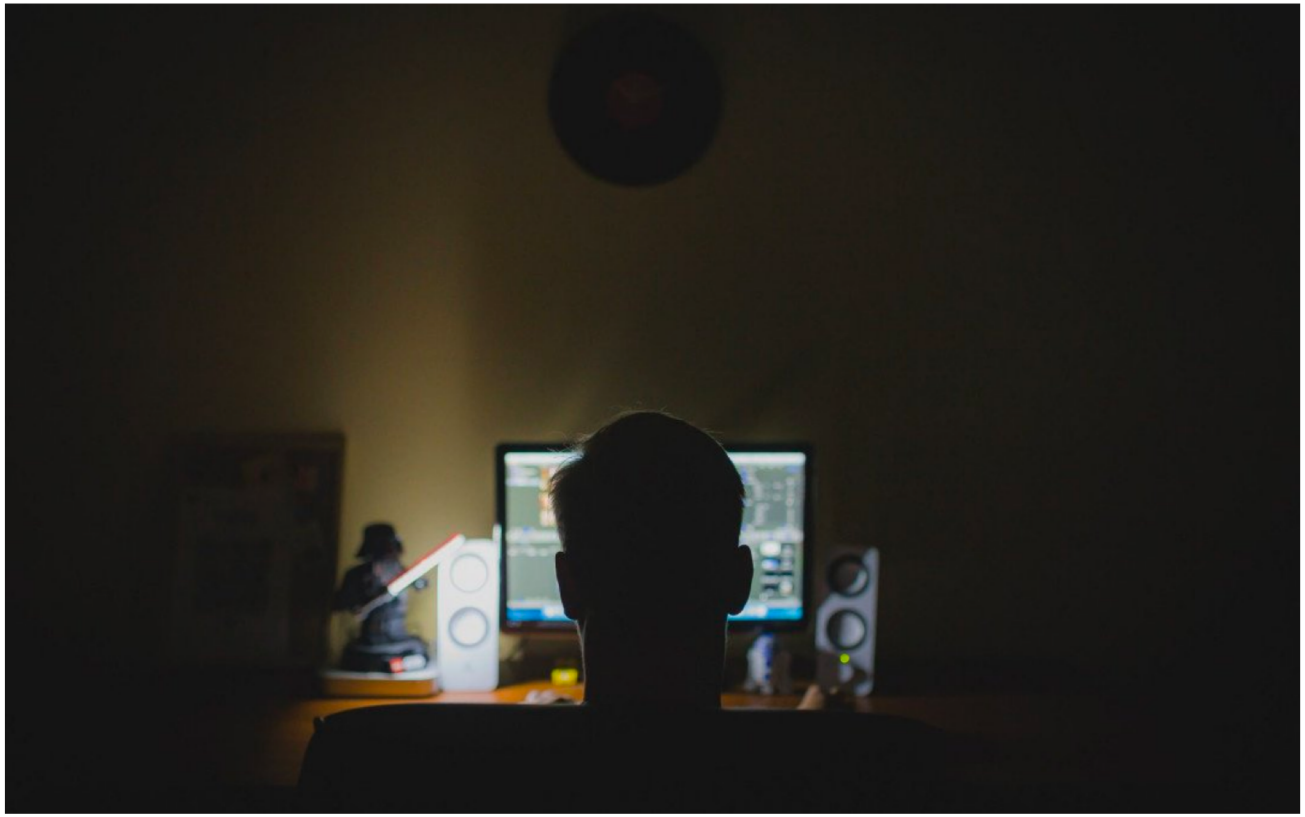
Design Choices – User Decisions



https://usabilla.com/blog/error-messages/

CASE STUDY - PASSWORDS

Home › ID Agent Blog › 63% of Data Breaches Result From Weak or Stolen Passwords



63% of Data Breaches Result From Weak or Stolen Passwords

https://info.idagent.com/blog/2017/06/16/63-data-breaches-result-weak-stolen-passwords

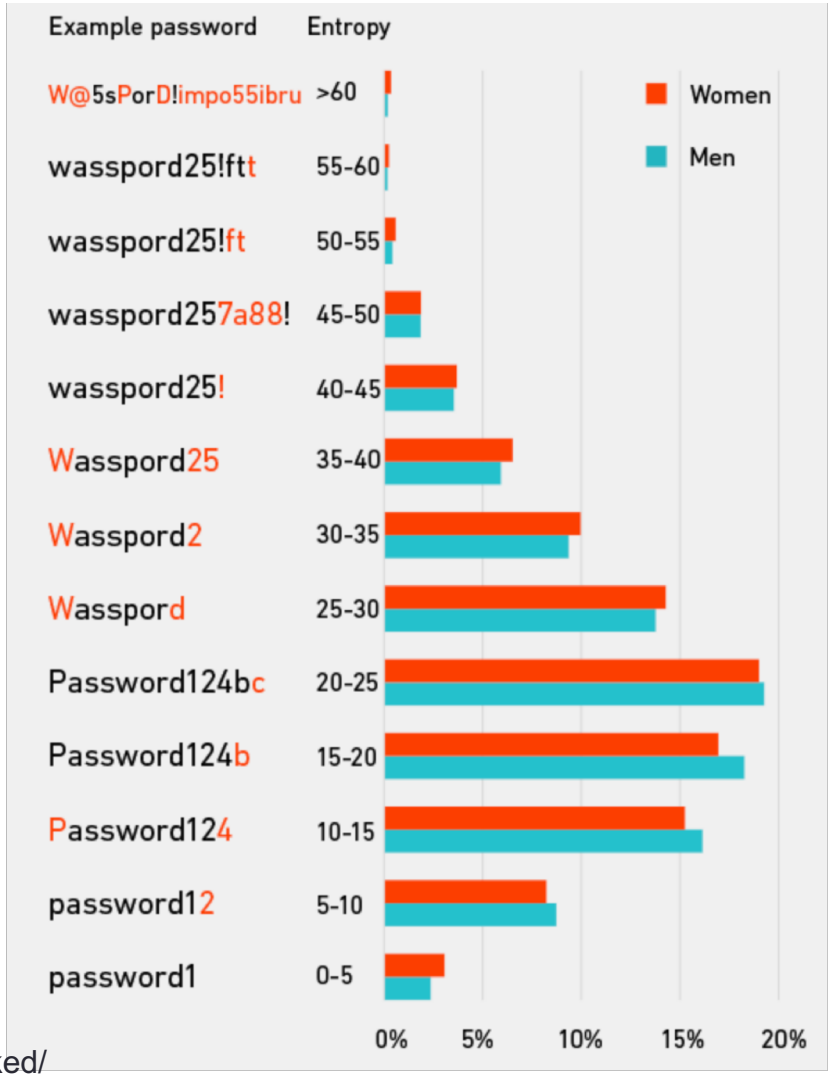
Study – most used passwords

https://wpengine.com/unmasked/

Evaluating password strength

- The more entropy a password has, the stronger it tends to be.
- Entropy increases with:
  - Increased length of the password
  - The variation of the characters that comprise it.

Entropy study of 485K users



https://wpengine.com/unmasked/

Estimating Password Strength

- Pasword Strength Calculator

Password Hacking

- How are password hacks?
  - Many users share their passwords with friends/family
  - Some passwords can be guessed
    - E.g. dog's name, birthday that's shared on Facebook, etc.
  - Brute force attack
    - Try all possible guesses
      - Choose with more common passwords
    - Start with a list of common words
    - Start with a list of most common passwords
  - Dictionary Attacks
    - Use the full dictionary of words

Passwords

- How to choose secure passwords?
  - Pick a strong password
    - Combination of different types of characters
  - Don’t reuse the password
  - Don’t write passwords down
  - Choose a hard to guess passwords
    - Don’t choose birthdays, friends’ names, etc.
  - Change passwords often

Passwords

- Typical user has many accounts
  - Needs to remember passwords for each

https://blog.centrify.com/stolen-passwords-mfa-saml/passwords-on-sticky-notes-small/

Passwords

- Alternative solutions exist
  - Combine security and usability
  - Example: graphical passwords longer meaningful passwords

Graphical passwords

- Security:
  - Need to ensure password space large enough
  - Passwords should be stored securely
- HCI:
  - User needs to be able to choose the password
    - Passwords should not be predictable
  - Passwords should be memorable
  - System should be usable
    - User willing to use it instead of regular passwords

Graphical passwords

Position-Based

https://www.usenix.org/legacy/publications/library/proceedings/sec04/tech/full_papers/davis/davis_html/node3.htm
https://flylib.com/books/en/2.176.1.51/1/

Longer Passwords

- Using phrases made up of a few common words may create a stronger and more usable password
  - Example: I love my dog
- Why is this option not popular?

COURSE GOALS

Main goals of the course

- Learn the importance of usability for security and privacy
- Current research in Cybersecurity
- How to design and execute usability studies
  - Iterative design, work as a team, communicate progress and results

Course Format

- Interactive lectures
- Course project
- Homework and readings
- All materials will be posted online

Course Format

- Class participation is encouraged
  - Raise your hand during class discussions and participate
  - Share interesting privacy/security news

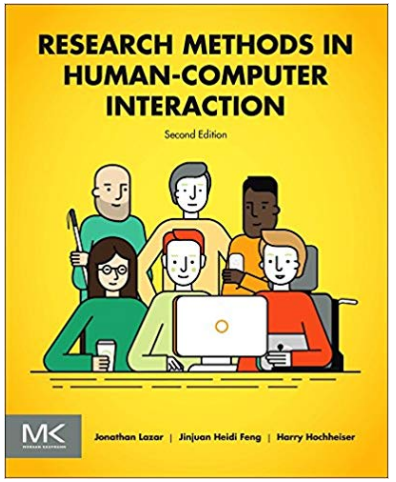
HCI course and CS Program

- Most courses teach technology – software/hardware
  - Operating systems, architecture, databases etc.
- This course introduces design & evaluation
  - Technology as a tool to evaluate via prototyping
  - Skills will become very important upon graduation
    - Complex systems, large teams
    - Other CS courses impact may not be as immediate

Project Description

- Design, conduct, and analyze a privacy or security user study
- Groups assigned based on your preferences
  - Work with students w/different skills/interests
- Deliverables: Project proposal, progress report and presentation, final presentation

Reading



- Textbook: Lazar et al.’s Research Methods in Human-Computer Interaction, 2 nd edition
- Complete readings before class

Class Policies

- Late homework/project: reduced credit
- Never share homework, solutions, code, etc.,
- Work on your own
  - unless assignment states otherwise
- Properly cite references used in your work
- CUNY full academic policy is available at:
  - CUNY Academic Integrity Policy

PRIVACY

Security and Privacy

- Security and privacy interconnected
  - In today's digital world
    - Internet of things, big data
- We will look at both

https://teachprivacy.com/opm-data-breach-fallout-fingerprints-and-other-privacy-security-updates/

Privacy

- What does privacy mean to you?
- Can you describe it in a few sentences or draw a picture?
- Share you description with the class

Privacy

- User tend to underestimate privacy risks from leaked data
- Recent headlines made users more aware of risks

3 related articles

Facebook users are changing their social habits amid privacy concerns

A survey says half of US users adjusted their privacy settings in the last year.

Mallory Locklear, @mallorylocklear
09.05.18 in Internet

8 Comments

255 Shares

https://www.engadget.com/2018/09/05/facebook-changing-social-habits-privacy-concerns/

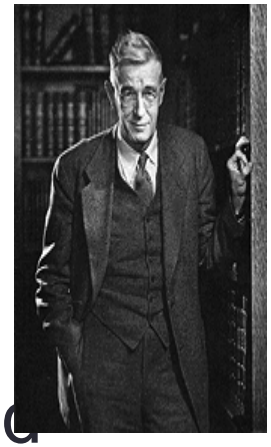
Privacy

- User tend to underestimate privacy risks from leaked data
- Recent headlines made users more aware of risks
- How can we protect users?
  - Providing privacy while maintaining usability?

Questions?

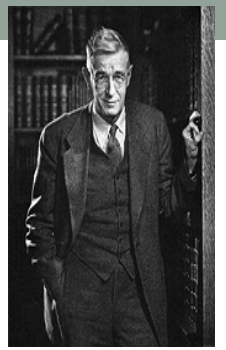
HCI HISTORY

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.)

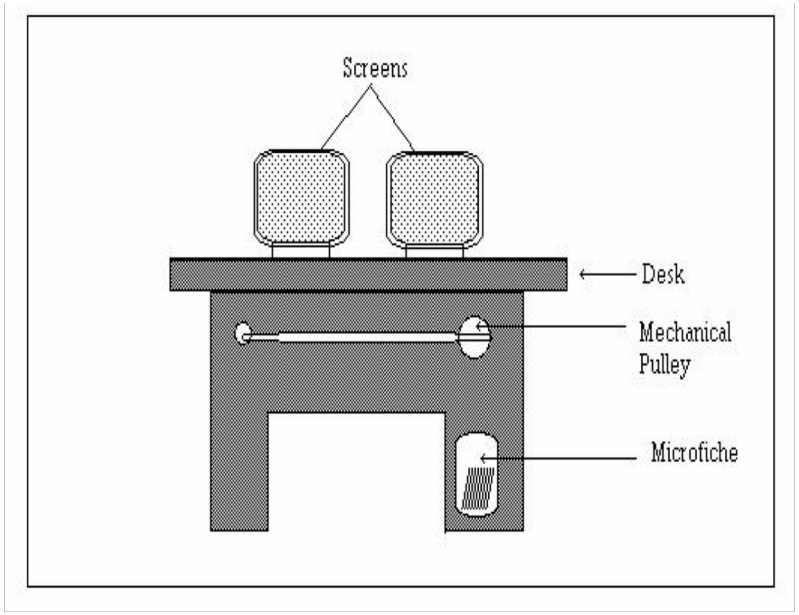


- Wrote "As We May Think" in 1945
  - A visionary description of the potential use for information technology
    - wearable cameras for photographic records
    - Encyclopedia Britannica for a nickel
    - automatic transcripts of speech
    - trails of discovery
    - direct capture of nerve impulses
    - Memex
  - Inspiring creators of the internet
    - Licklider Engelbart, etc.
      - Although Memex was never created

"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



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
- A device in which an individual stores all his books, records, and communications
  - mechanized so that it may be consulted with exceeding speed and flexibility
- 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

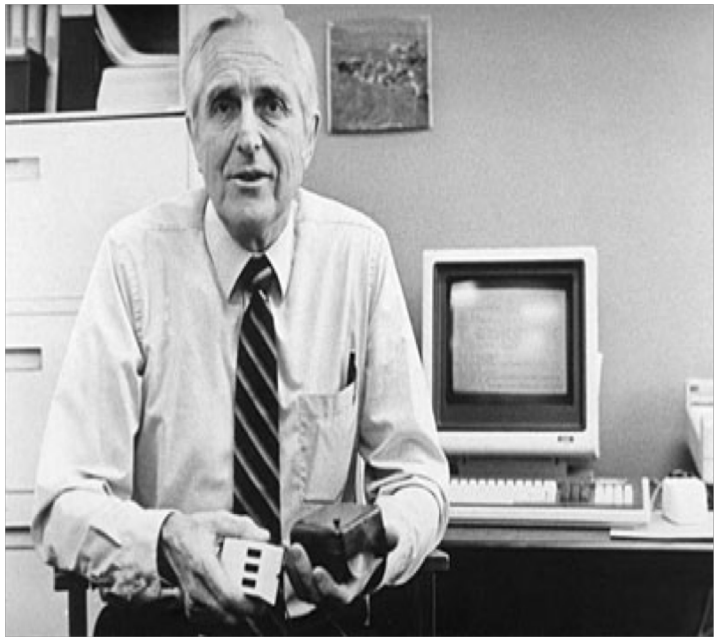
Augmenting Human Intellect

- 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

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."

Summary

- Computers do not need to be the way we see them today
- Predict the future by inventing it
- Your vision is the key
  - Human factor is an important factor in system design!

Questions?