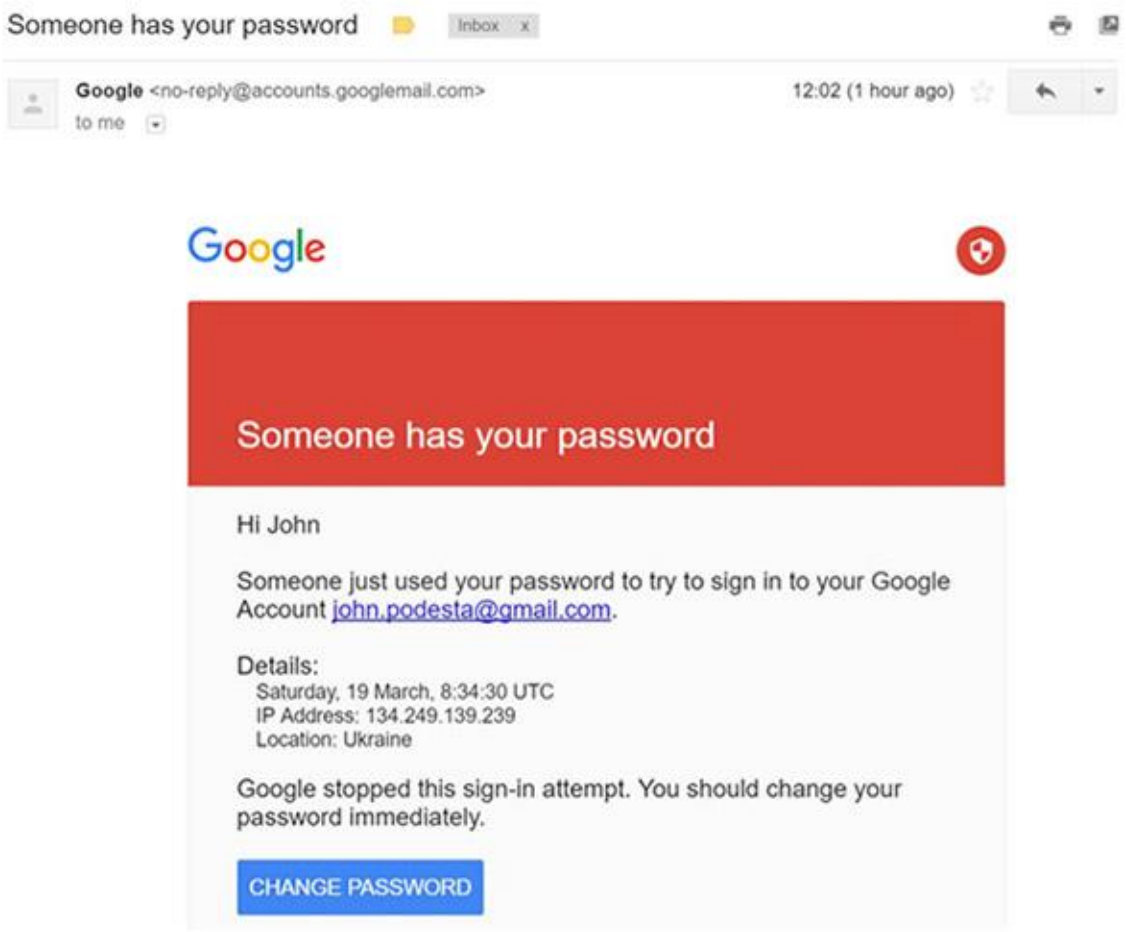
05. Phishing; Robust and Ethical Experiments

Blase Ur
April 16th, 2019
CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO

Security, Usability, & Privacy Education & Research

Why John Can’t Protect His Emails



Phishing

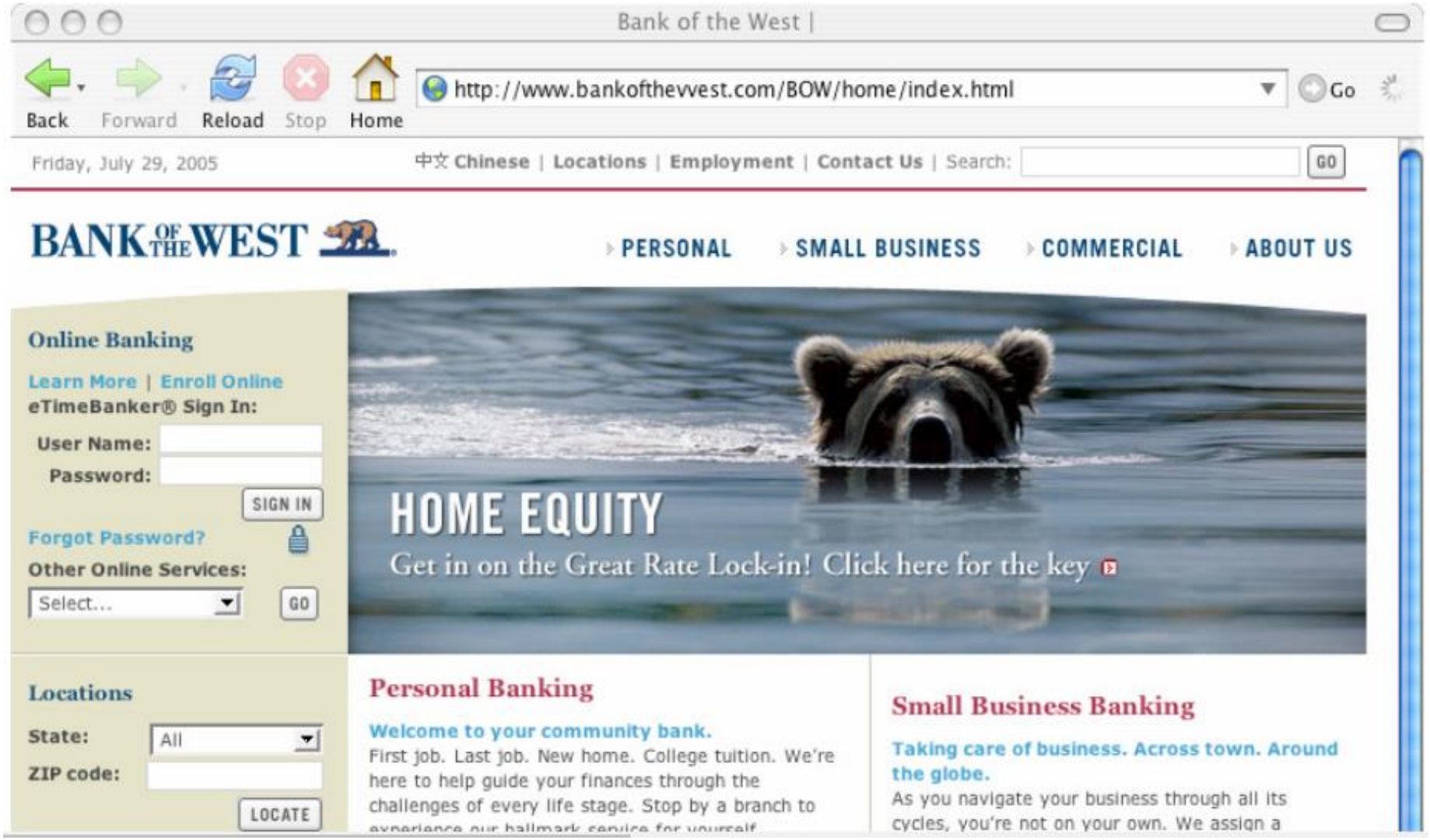
- Phish: Fraudulent email that looks real
  - Usually try to extract credentials (e.g., password), financial information (e.g., bank account), or other private information
- Spear phish: Targeted phishing email

Why Does Phishing Work?

- Rachna Dhamija, J.D. Tygar, Marti Hearst. Why Phishing Works. CHI 2006.
- How do you tell if a site is legitimate?
- How do you tell if an email is legitimate?

Legitimate or Phish?

Legitimate or Phish?



Anti-Phishing Phil / PhishGuru

Social phishing (Jagatic et al., 2007)

- Use social networking sites to get information for targeted phishing
  - "In the study described here we simply harvested freely available acquaintance data by crawling social network Web sites."
- "We launched an actual (but harmless) phishing attack targeting college students aged 18–24 years old."

Social phishing (Jagatic et al., 2007)

- Control group: message from stranger
- Experimental group: message from a friend
- Used university's sign-on service to verify passwords phished

Ethics (Jagatic et al., 2007)

- How did they obtain consent?
- What ethical concerns are there?
  - What seemed to be done well?
  - What could have been done better?
- Who was potentially affected by the study?
- "The number of complaints made to the campus support center was also small (30 complaints, or 1.7% of the participants)."

HCI Experimental Methods

Human-Computer Interaction (HCI)

- You are not the user! You know too much!
- Think about the user throughout design
- Involve the user

What is usable?

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

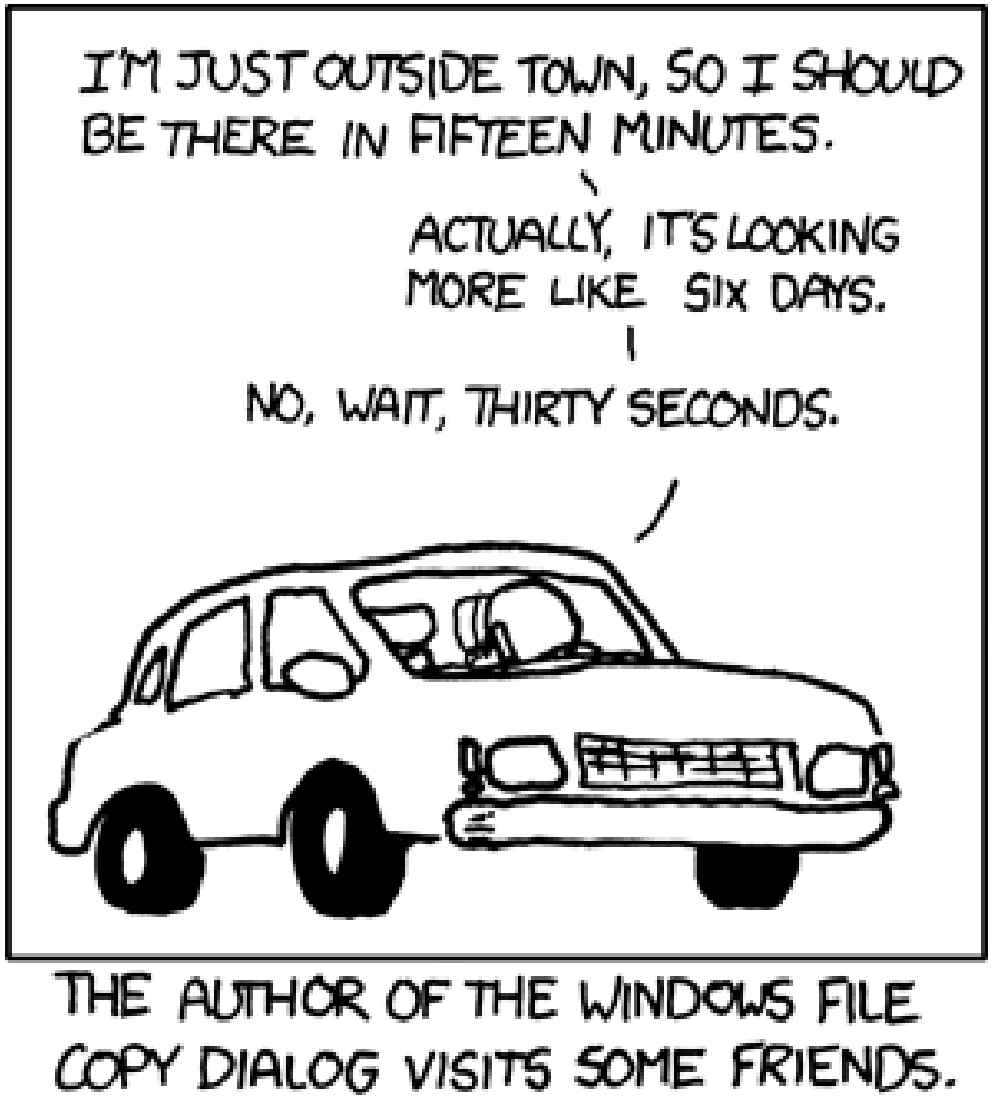


Image from http://www.xkcd.com

Determine use cases and goals

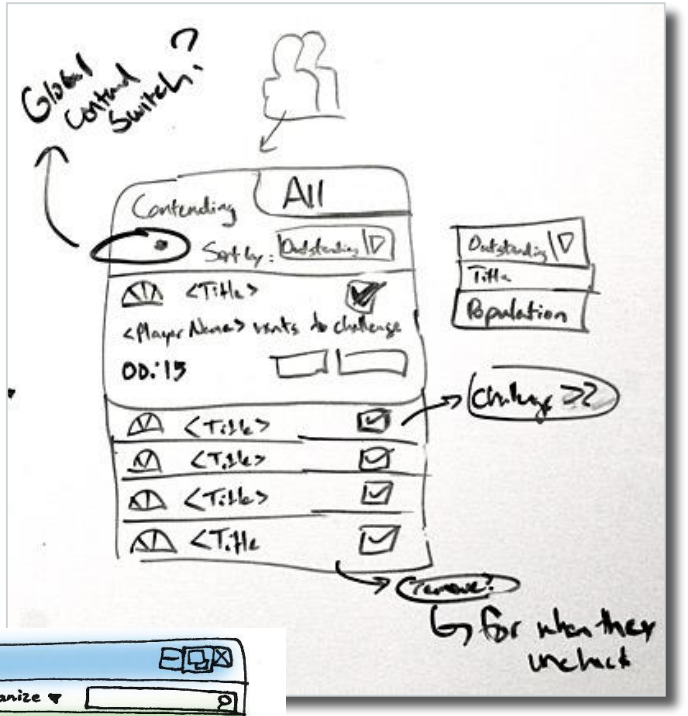
- What are the concrete tasks users should be able to accomplish?
  - Based on understanding of users!
- Set realistic metrics

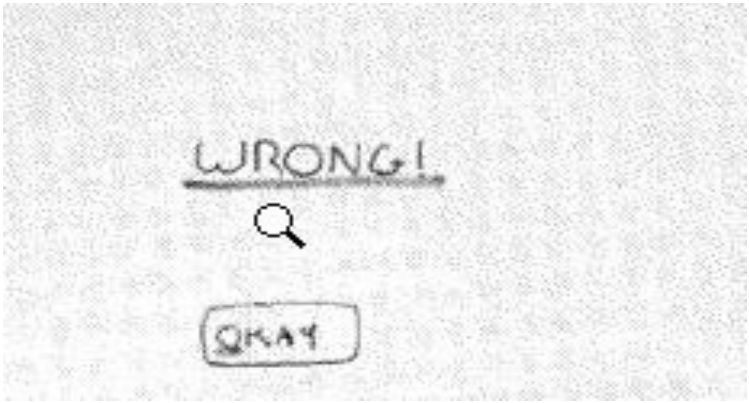
Example: paper prototypes

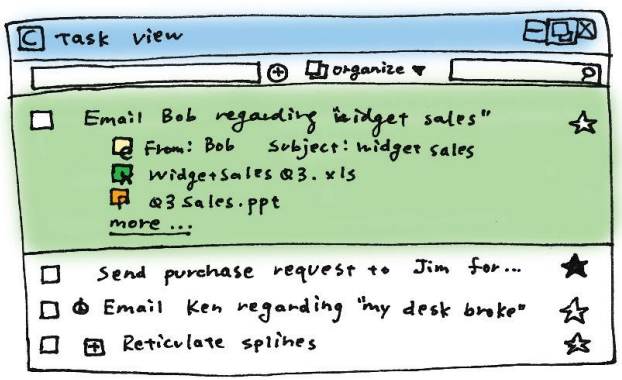
- Don’t overthink. Just make it.
- Draw a frame on a piece of paper
- Sketch anything that appears on a card
- Make all menus, etc.
- Redesign based on feedback
- “Think aloud”

Iterative prototyping is crucial!

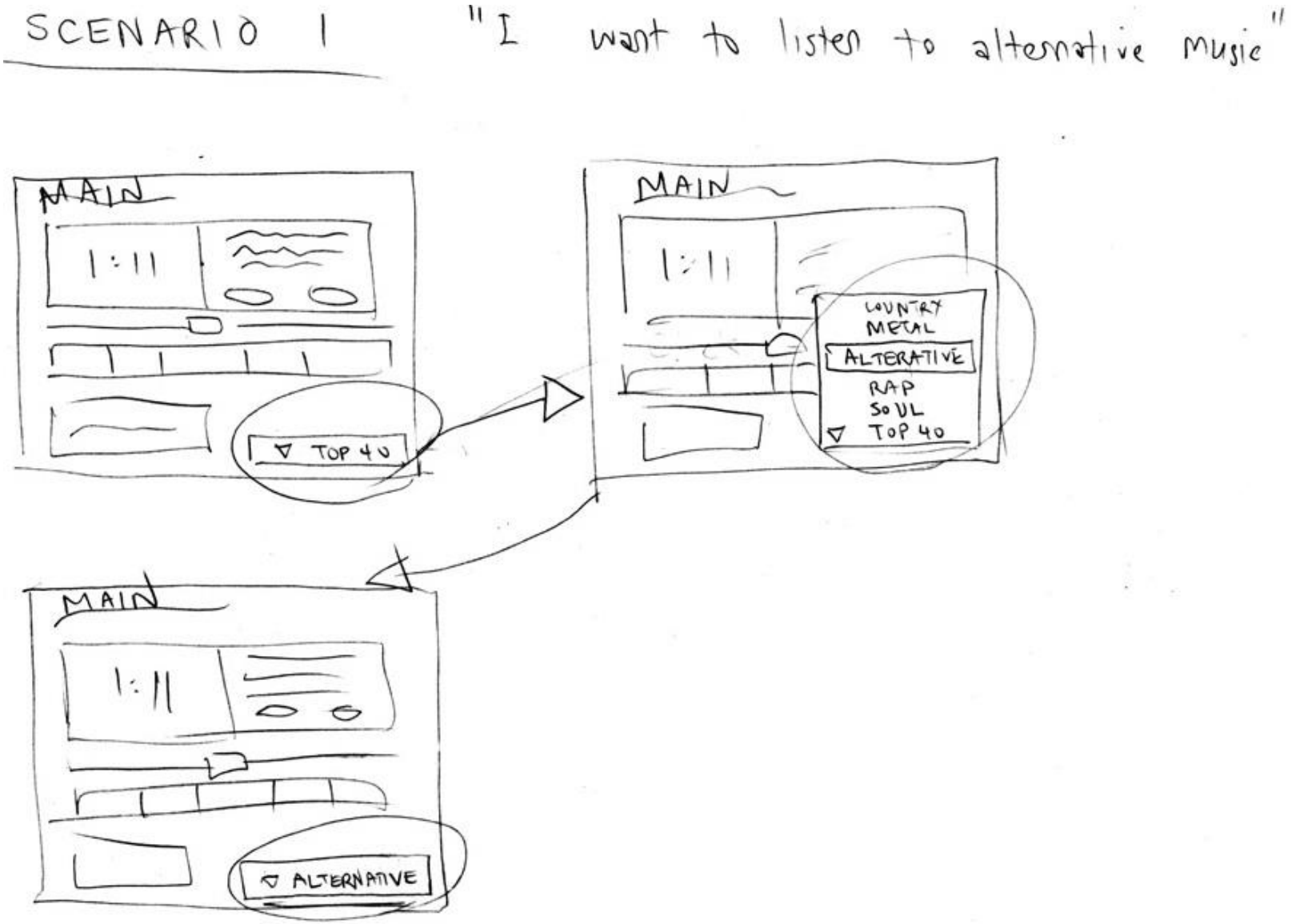
High-fidelity, “Wizard of Oz,” low-fidelity



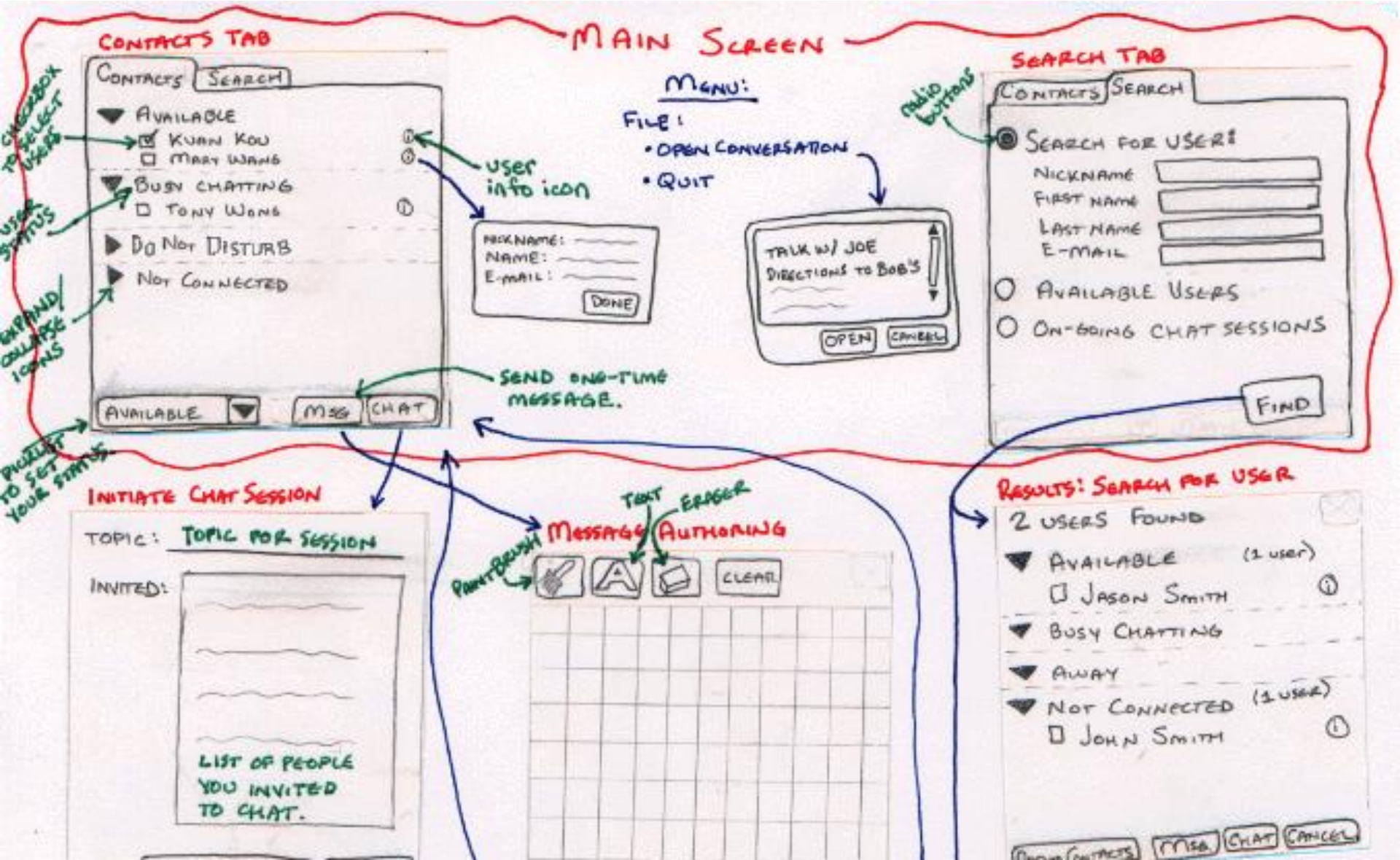




Example: low-fidelity paper prototype



Example: paper prototype



Example: think aloud

- Download and install software that lets you encrypt your email
  - "Think aloud" of whatever's on your mind
  - Give them an example

- Additional things you can ask:
  - What are you thinking now?
  - What do you expect to happen if you do X?
  - How did you decide to do that?

Research Studies and Methods

Research studies: purpose and goals

- What are you hoping to learn?
- What are your hypotheses?
  - Often listed explicitly in a paper
- What are your metrics for success?
  - More secure, quicker to use, more fun, etc.
- What are you comparing to?
- What data might be helpful?

Broad types of studies

- Descriptive study
- Relational study
- Experimental study
- Formative (initial) vs. summative (validate)

Quantitative vs. Qualitative

- Quantitative: you have numbers (timing data, ratings of awesomeness)
- Qualitative: you have non-numerical data (thoughts, opinions, types of errors)

Types of studies (1)

- What people want/think/do overall:
  - Surveys
  - Interviews
  - Focus groups
- What people want/think in context:
  - Contextual inquiry (interviews)
  - Diary study (prompt people)
  - Observations in the field

Types of studies (2)

- Expert evaluation of usability:
  - Cognitive walkthrough
  - Heuristic evaluation
- Usability test:
  - Laboratory (“think aloud”)
  - Online study
  - Log analysis

Types of studies (3)

- Controlled experiments to test causation
- Varying different conditions
  - Full-factorial design or not
  - Independent and dependent variables
- Many methods apply (e.g., surveys can be designed to test causation)
  - Role-playing studies
  - Field studies

Study designs

- Within subjects
  - Every participant tests everything
  - Crucial to randomize order! (learning effect)
  - Fewer participants
- Between subjects
  - Each participant tests 1 version of the system
  - You compare these groups
  - Groups should be similar (verify!)
  - Still randomize!