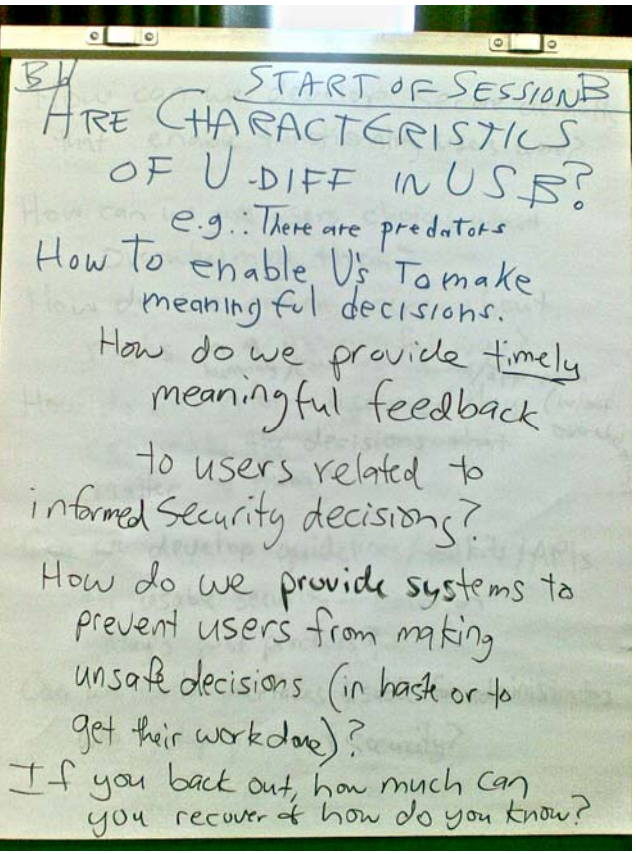
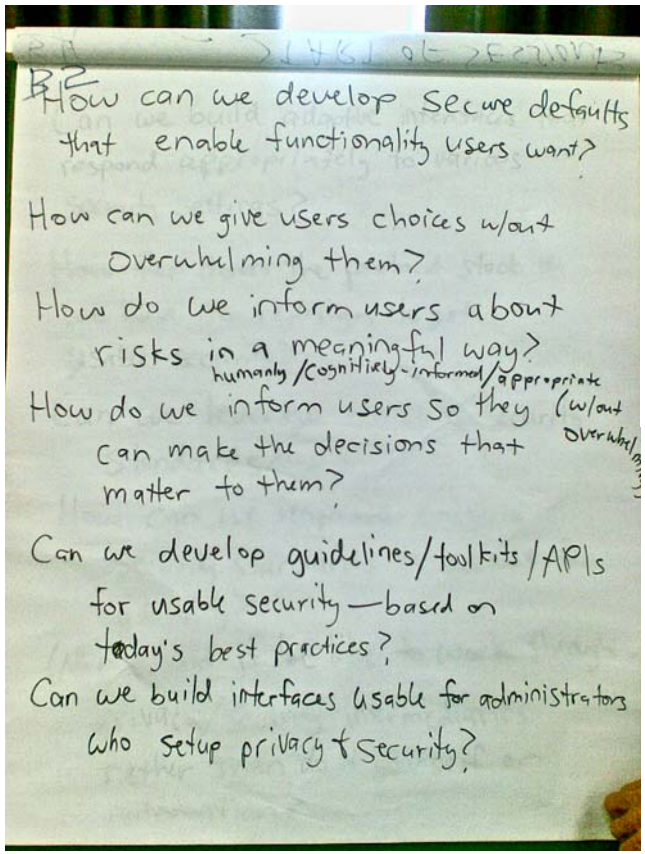
Session Summary
Approaches to Usable Security

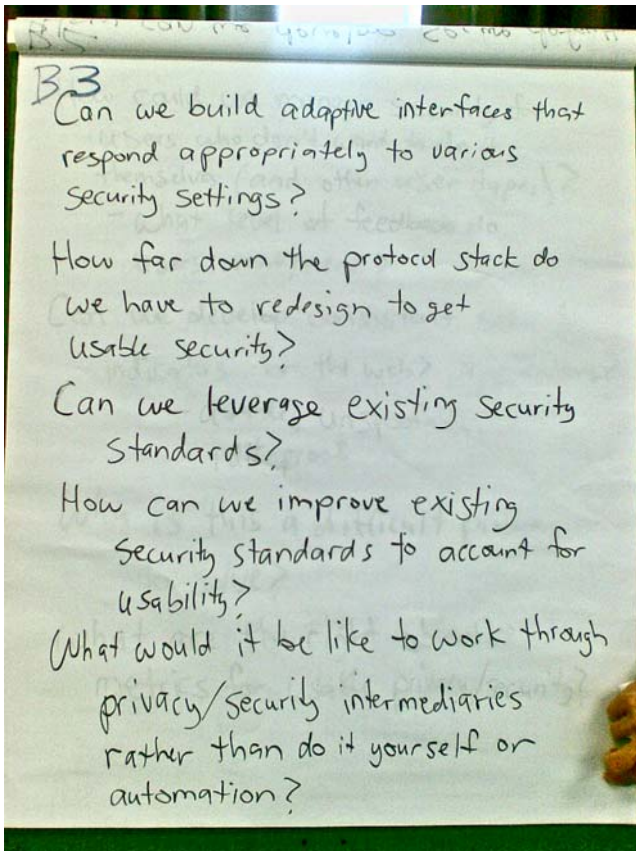
Lorrie Cranor

Don Norman

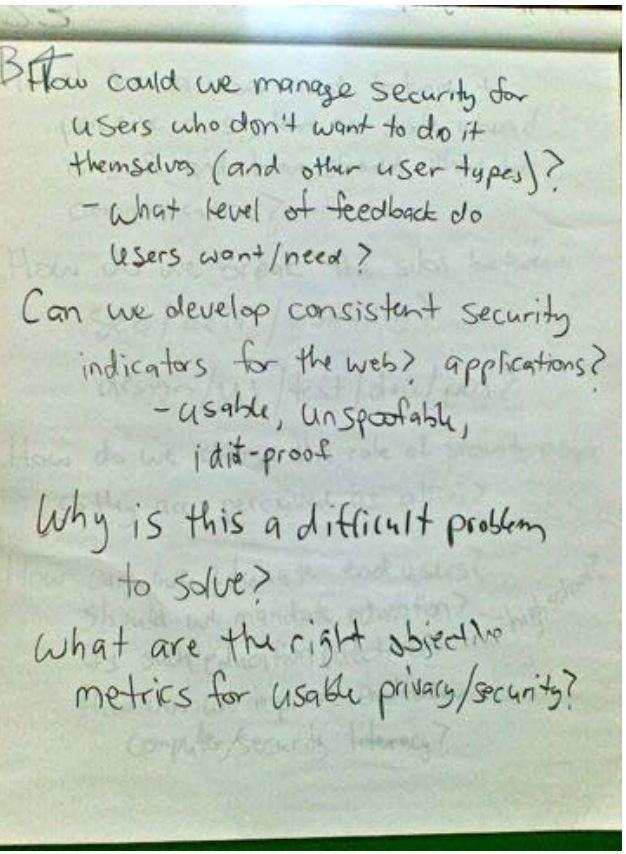
Approaches to Usable Security Session Notes

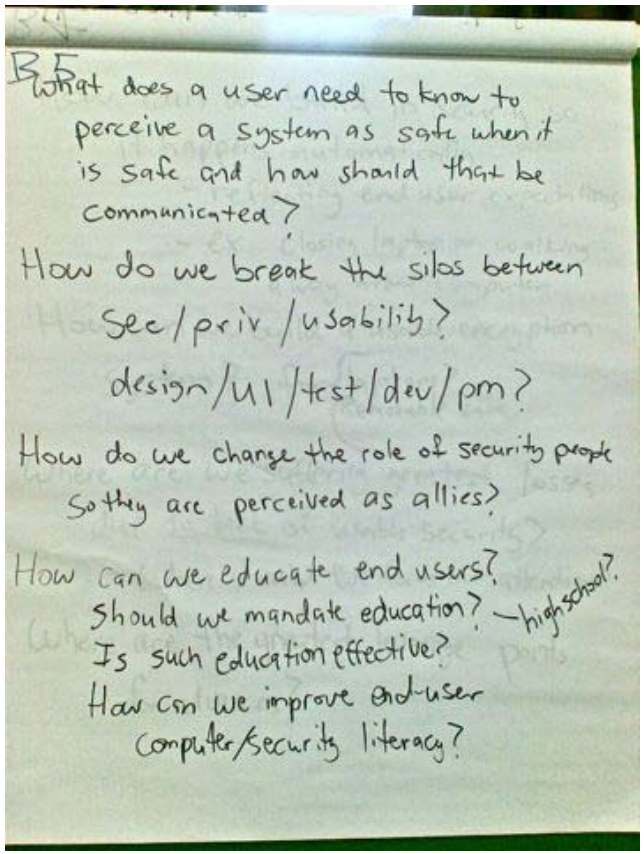


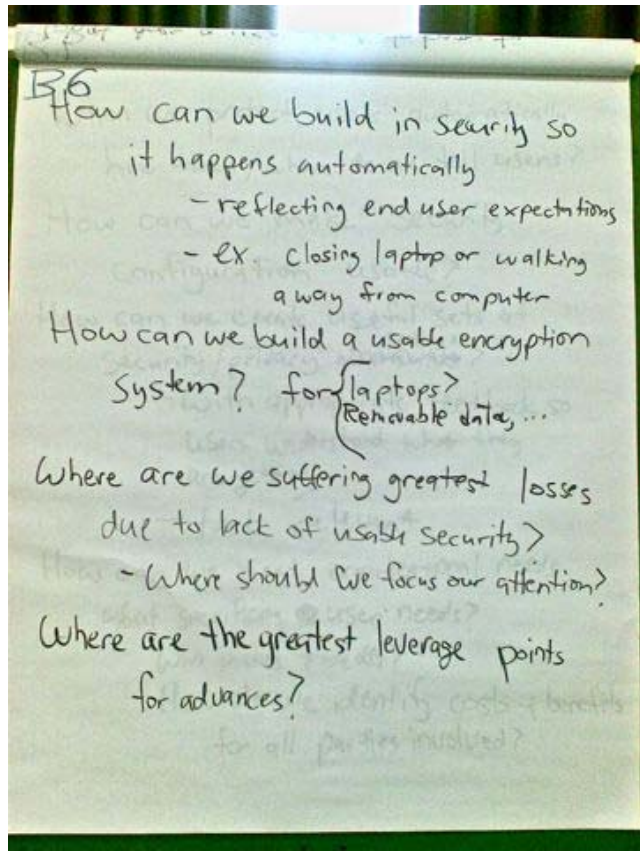




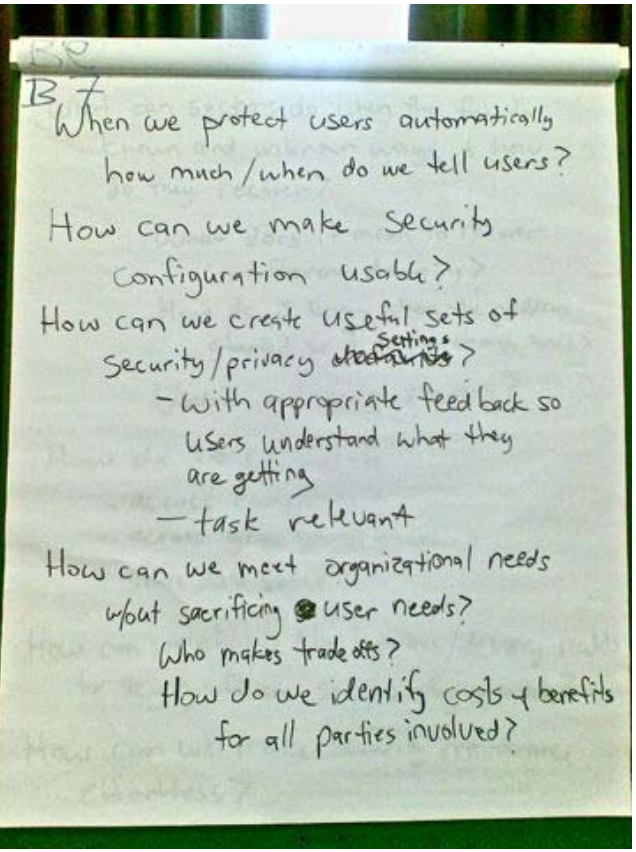
Approaches to Usable Security Session Notes

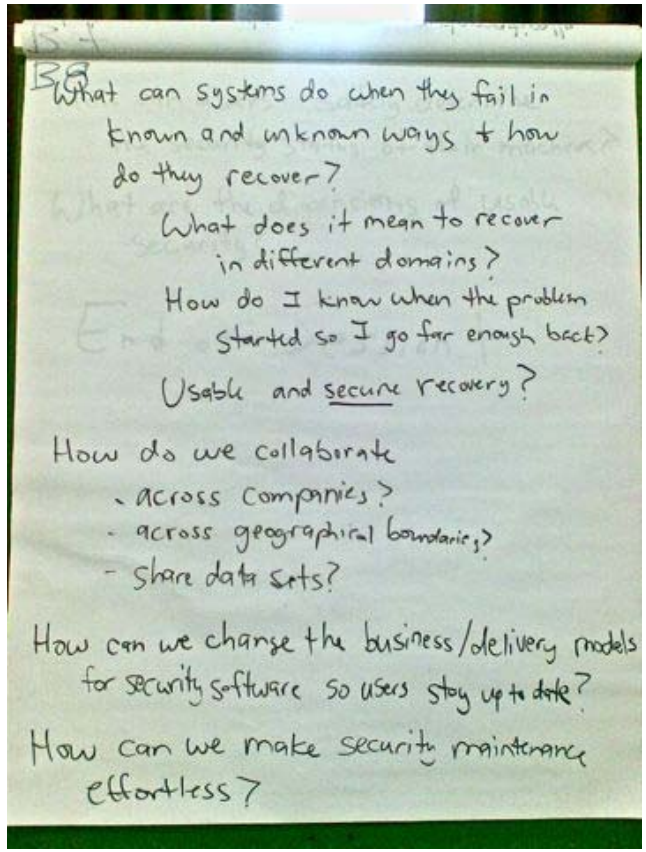


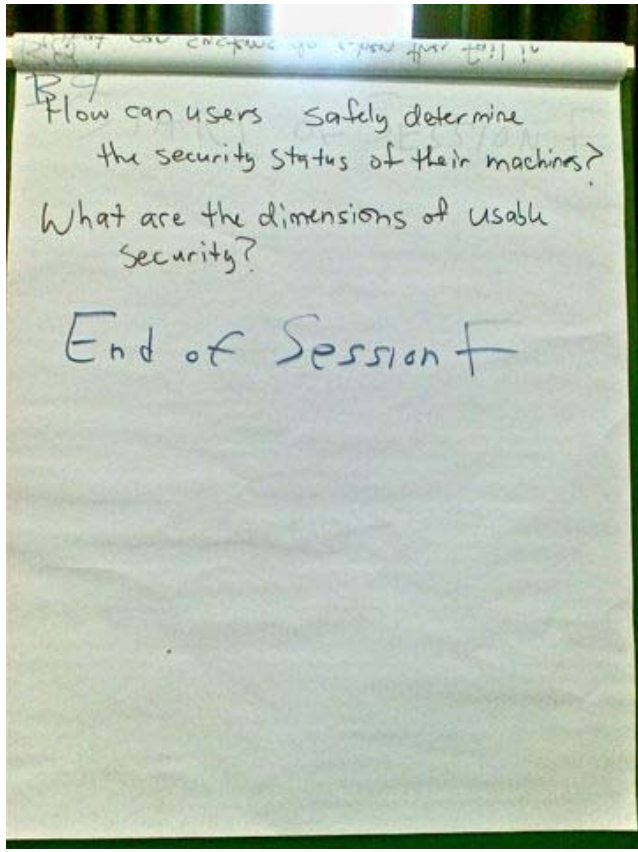




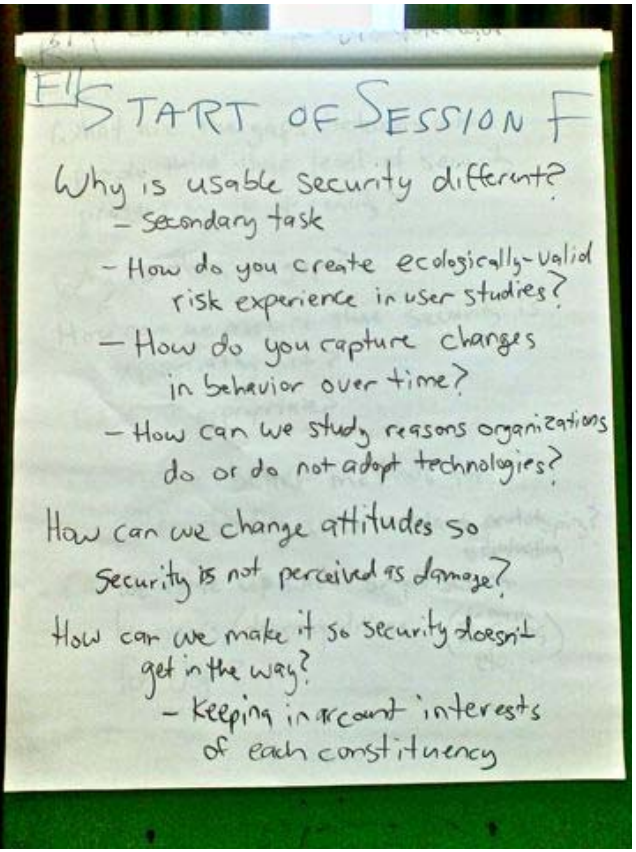
Approaches to Usable Security Session Notes

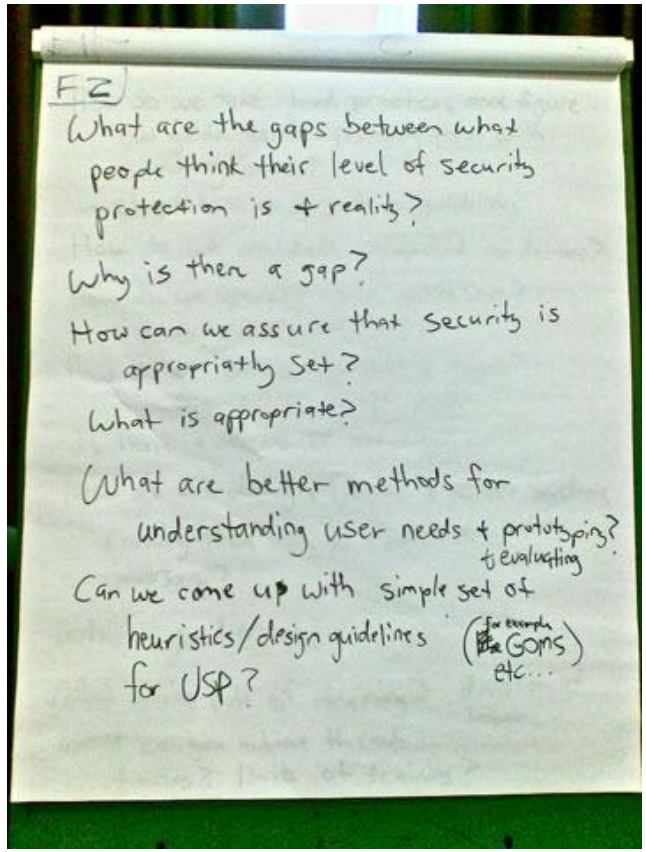


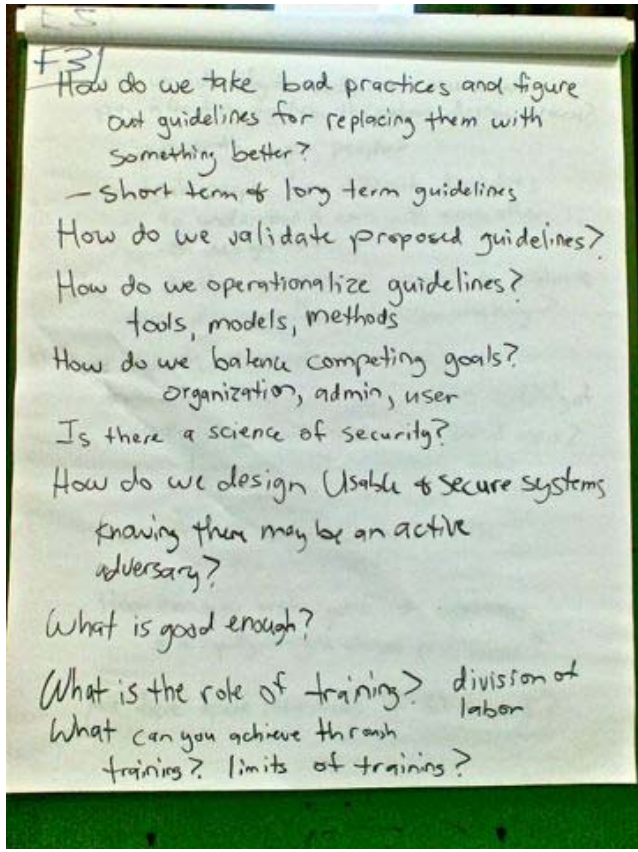




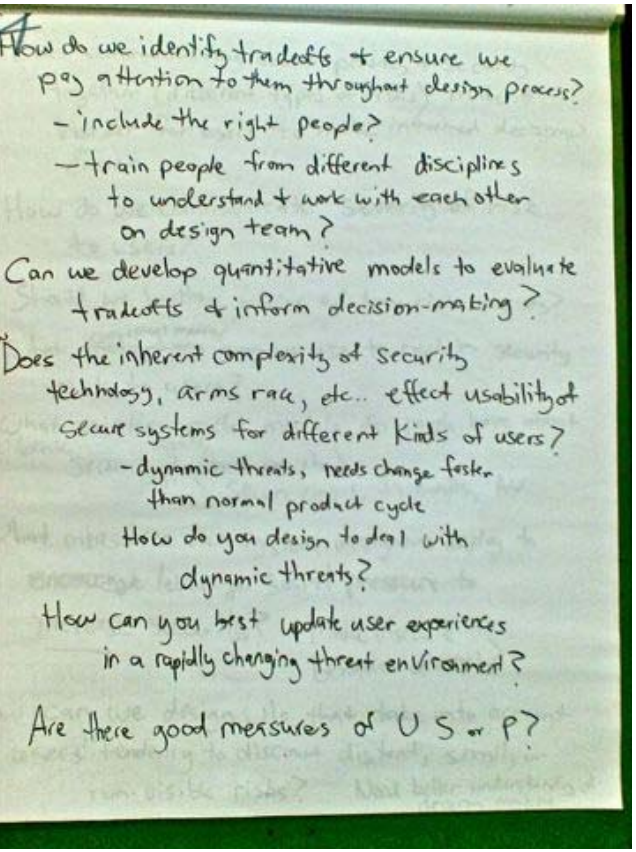
Approaches to Usable Security Session Notes

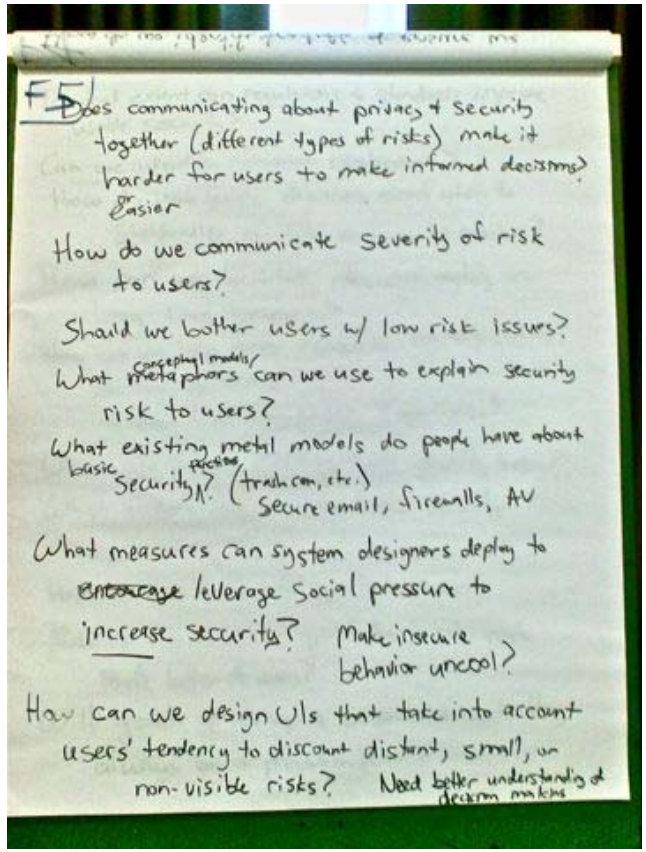


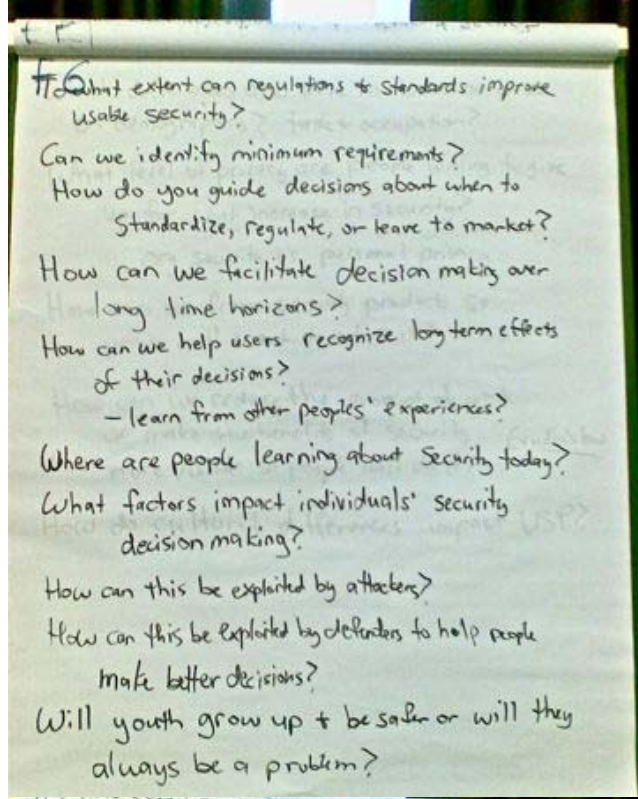


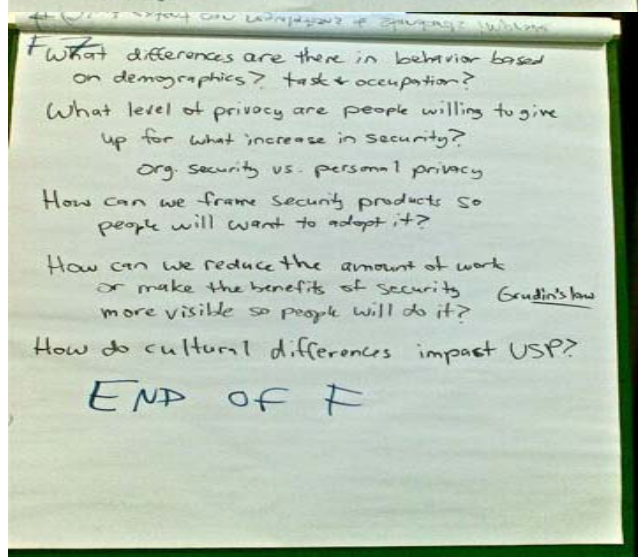


Approaches to Usable Security Session Notes









Business models

Standards and regulations

What are dimensions of usable security?

communication

Is USB special

Metrics

Developer support

Human behavior

Feedback about security decisions

Administrative tools

Training and education

Prioritization

Bundles of settings

Design process

Recovery

Automation

Human-centered design

Costs and benefits: tradeoffs

Internet/infrastructure/OS redesign

Shared data sets

Is USP special

Business models

Prioritization

Costs and benefits: tradeoffs

Standards and regulations

What are dimensions of usable security?

Metrics

Shared data sets

Developer support

Design process

Bundles of settings

Recovery

Administrative tools

Internet/infrastructure/OS redesign

Human-centered design

Human behavior

communication

Feedback about security decisions

Automation

Training and education

Understanding USP

- What are the dimensions of usable security and privacy?
  - Prioritization – where can we have greatest impact?
- Is usable security and privacy special?
  - How? (active adversary, secondary, hard to study)
  - How is it similar to other usability domains and what can we learn from them?
- How to influence development of more usable security?
  - Change business models so security subscriptions never expire
  - Standards and regulations
- How to evaluate usability and security?
  - Metrics
  - Shared data sets
  - Costs and benefits of security, tradeoffs

Approaches to USP

- Automation
  - Ex: How can we build usable encryption systems?
- User education
  - Role of education, limits of education
  - Should it be mandated?
  - What do users already know and how did they learn it?
- Human-centered design
  - Feedback and communication
  - Explicit conceptual model
  - Informed by observation of human behavior
    - Demographic/cultural differences
    - What tradeoffs will people make and how do we influence them?

Processes and tools

- Developer support tools
  - Guidelines, principles, design patterns, heuristics
  - Short term, based on what we know now
  - Long term research questions
  - How do we validate?
- Design process
  - Removing silos, training people from different disciplines to work together
  - How to deal with dynamic threats that develop between design iterations?
- Recovery
  - How do we recover from security problems in different applications?
  - How can we make recovery secure and usable?
- Administrative tools
  - Help administrators work on behalf of users
- Simplify user decisions
  - Bundles of settings
  - Secure defaults
- Internet/infrastructure/OS redesign