

# Session Summary

## Approaches to Usable Security

Lorrie Cranor

Don Norman

# Approaches to Usable Security Session Notes

B1 START OF SESSION  
ARE CHARACTERISTICS  
OF U-DIFF IN US?  
e.g.: There are predators  
How to enable U's to make  
meaningful decisions.  
How do we provide timely  
meaningful feedback  
to users related to  
informed security decisions?  
How do we provide systems to  
prevent users from making  
unsafe decisions (in haste or to  
get their work done)?  
If you back out, how much can  
you recover & how do you know?

B2  
How can we develop secure defaults  
that enable functionality users want?  
How can we give users choices w/out  
overwhelming them?  
How do we inform users about  
risks in a meaningful way?  
humanly/cognitively-informed/appropriate  
How do we inform users so they (w/out  
overwhelm)  
can make the decisions that  
matter to them?  
Can we develop guidelines/toolkits/APIs  
for usable security—based on  
today's best practices?  
Can we build interfaces usable for administrators  
who setup privacy & security?

B3  
Can we build adaptive interfaces that  
respond appropriately to various  
security settings?  
How far down the protocol stack do  
we have to redesign to get  
usable security?  
Can we leverage existing security  
standards?  
How can we improve existing  
security standards to account for  
usability?  
(What would it be like to work through  
privacy/security intermediaries  
rather than do it yourself or  
automation?)

# Approaches to Usable Security Session Notes

B How could we manage security for users who don't want to do it themselves (and other user types)?  
- What level of feedback do users want/need?  
Can we develop consistent security indicators for the web? applications?  
- usable, unspoofable, idit-proof  
Why is this a difficult problem to solve?  
What are the right objective metrics for usable privacy/security?

B What does a user need to know to perceive a system as safe when it is safe and how should that be communicated?  
How do we break the silos between Sec/priv/usability?  
design/UI/test/dev/pm?  
How do we change the role of security people so they are perceived as allies?  
How can we educate end users?  
Should we mandate education? - high school?  
Is such education effective?  
How can we improve end-user computer/security literacy?

B How can we build in security so it happens automatically  
- reflecting end user expectations  
- ex. closing laptop or walking away from computer  
How can we build a usable encryption system? for {laptops? Renewable data, ...}  
Where are we suffering greatest losses due to lack of usable security?  
- Where should we focus our attention?  
Where are the greatest leverage points for advances?

# Approaches to Usable Security Session Notes

B7  
When we protect users automatically  
how much/when do we tell users?  
How can we make security  
configuration usable?  
How can we create useful sets of  
security/privacy <sup>Settings</sup> ~~choices~~?  
- with appropriate feedback so  
users understand what they  
are getting  
- task relevant  
How can we meet organizational needs  
w/out sacrificing user needs?  
Who makes trade offs?  
How do we identify costs & benefits  
for all parties involved?

B7  
What can systems do when they fail in  
known and unknown ways & how  
do they recover?  
What does it mean to recover  
in different domains?  
How do I know when the problem  
started so I go far enough back?  
Usable and secure recovery?  
How do we collaborate  
- across companies?  
- across geographical boundaries?  
- share data sets?  
How can we change the business/delivery models  
for security software so users stay up to date?  
How can we make security maintenance  
effortless?

B7  
How can users safely determine  
the security status of their machines?  
What are the dimensions of usable  
security?  
End of Session f

# Approaches to Usable Security Session Notes

## F1 START OF SESSION F

Why is usable security different?

- secondary task
- How do you create ecologically-valid risk experience in user studies?
- How do you capture changes in behavior over time?
- How can we study reasons organizations do or do not adopt technologies?

How can we change attitudes so security is not perceived as damage?

How can we make it so security doesn't get in the way?

- keeping in account interests of each constituency

## F2

What are the gaps between what people think their level of security protection is + reality?

Why is there a gap?

How can we assure that security is appropriately set?

What is appropriate?

What are better methods for understanding user needs + prototyping?

Can we come up with simple set of heuristics/design guidelines (for example the GOMS) etc...  
for USP?

## F3

How do we take bad practices and figure out guidelines for replacing them with something better?

- short term + long term guidelines

How do we validate proposed guidelines?

How do we operationalize guidelines?  
tools, models, methods

How do we balance competing goals?  
organization, admin, user

Is there a science of security?

How do we design Usable + Secure systems knowing there may be an active adversary?

What is good enough?

What is the role of training? division of labor  
What can you achieve through training? limits of training?

# Approaches to Usable Security Session Notes

How do we identify tradeoffs + ensure we pay attention to them throughout design process?

- include the right people?
- train people from different disciplines to understand + work with each other on design team?

Can we develop quantitative models to evaluate tradeoffs + inform decision-making?

Does the inherent complexity of security technology, arms race, etc.. effect usability of secure systems for different kinds of users?

- dynamic threats, needs change faster than normal product cycle

How do you design to deal with dynamic threats?

How can you best update user experiences in a rapidly changing threat environment?

Are there good measures of U S or P?

F5 Does communicating about privacy + security together (different types of risks) make it harder for users to make informed decisions?  
Easier

How do we communicate severity of risk to users?

Should we bother users w/ low risk issues?

What <sup>conceptual models/</sup> metaphors can we use to explain security risk to users?

What existing mental models do people have about <sup>basic</sup> security? (trash can, etc.)  
Secure email, firewalls, AV

What measures can system designers deploy to ~~encourage~~ leverage social pressure to increase security?  
Make insecure behavior uncool?

How can we design UIs that take into account users' tendency to discount distant, small, or non-visible risks? Need better understanding of decision making

F6 What extent can regulations + standards improve usable security?

Can we identify minimum requirements?

How do you guide decisions about when to standardize, regulate, or leave to market?

How can we facilitate decision making over long time horizons?

How can we help users recognize long term effects of their decisions?

- learn from other peoples' experiences?

Where are people learning about security today?

What factors impact individuals' security decision making?

How can this be exploited by attackers?

How can this be exploited by defenders to help people make better decisions?

Will youth grow up + be safer or will they always be a problem?

F7 What differences are there in behavior based on demographics? task + occupation?

What level of privacy are people willing to give up for what increase in security?  
Org security vs. personal privacy

How can we frame security products so people will want to adopt it?

How can we reduce the amount of work or make the benefits of security more visible so people will do it? *Grudin's law*

How do cultural differences impact USP?

END OF F

Business models

What are dimensions of usable security?

Standards and regulations

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