Usable security and the human in the loop

Michelle Mazurek

Some slides adapted from Lujo Bauer, Lorrie Cranor, Rob Reeder, Blase Ur, and Yinqian Zhang
Today’s class

• Introducing me
• Introducing you
• Human Factors for Security and Privacy?
• Course policies and syllabus
• The human in the loop
Who am I?

• Michelle Mazurek (mmazurek@umd.edu)
• Assistant professor, CS and UMIACS
• Affiliated with MC2 and HCIL
• Office hours: Tues 2-3 pm in AVW 3421, or by appointment
Who are you?

• Preferred name
• Academic program, adviser if applicable
• Background in HCI (a lot, a little, none)
• Background in security/privacy (a lot, a little, none)
• Why this course?
“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.”

More on humans

“Not long ago, [I] received an e-mail purporting to be from [my] bank. It looked perfectly legitimate, and asked [me] to verify some information. [I] started to follow the instructions, but then realized this might not be such a good idea … [I] definitely should have known better.”

-- former FBI Director Robert Mueller
And one more …

“I think privacy is actually overvalued … If someone drained my cell phone, they would find a picture of my cat, some phone numbers, some email addresses, some email text. What’s the big deal?”

-- Judge Richard Posner
U.S. Court of Appeals, 7th circuit
Better together

Examining security/privacy and usability together is often critical for achieving either
Borrowing from many disciplines

Many disciplines have experience studying humans. Can we learn from their models and methods?

- Psychology
- Sociology
- Ethnography
- Cognitive sciences
- Warning science
- Risk perception
- Behavioral economics
- HCI
- Marketing
- Counterterrorism
- Communication
- Persuasive technology
- Learning science
Why is security/privacy different?

• Presence of an adversary
• Security/privacy is a secondary task
• Designing for humans is not enough!
  – Support users who are predictable, stressed, careless, unmotivated, busy, foolish
  – **Without** compromising security and privacy
## Bridging security and HCI

<table>
<thead>
<tr>
<th>Security</th>
<th>Usability/HCI</th>
<th>Usable Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humans are a secondary constraint compared to security concerns</td>
<td>Humans are the primary constraint, security is rarely considered</td>
<td>Human factors and security are both primary constraints</td>
</tr>
</tbody>
</table>
# Bridging security and HCI

<table>
<thead>
<tr>
<th>Security</th>
<th>Usability/HCI</th>
<th>Usable Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humans are a secondary constraint compared to security concerns</td>
<td>Humans are the primary constraint, security is rarely considered</td>
<td>Human factors and security are both primary constraints</td>
</tr>
<tr>
<td>Humans considered primarily in their role as adversaries/attackers</td>
<td>Concerned about human error but not human attackers</td>
<td>Concerned about both normal users and adversaries</td>
</tr>
<tr>
<td>Involves threat models</td>
<td>Involves task models, mental models, cognitive models</td>
<td>Involves threat models AND task models, mental models, etc.</td>
</tr>
<tr>
<td>Focus on security metrics</td>
<td>Focus on usability metrics</td>
<td>Considers usability and security metrics together</td>
</tr>
<tr>
<td>User studies are rare</td>
<td>User studies are common</td>
<td>User studies common, often involve deception or distraction</td>
</tr>
</tbody>
</table>
# User-selected graphical passwords

<table>
<thead>
<tr>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the space of possible passwords?</td>
</tr>
<tr>
<td>How can we make the password space larger to make the password harder to guess?</td>
</tr>
<tr>
<td>How are the stored passwords secured?</td>
</tr>
<tr>
<td>Can an attacker gain knowledge by observing a user entering her password?</td>
</tr>
</tbody>
</table>
# User-selected graphical passwords

<table>
<thead>
<tr>
<th>Security</th>
<th>Usability/HCI</th>
<th>Usable Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the space of possible passwords?</td>
<td>How difficult is it for a <strong>user</strong> to create, remember, and enter a graphical password? How long does it take? How hard is it for users to learn the system? Are users <strong>motivated</strong> to put in effort to create good passwords? Is the system <strong>accessible</strong> using a variety of devices, for users with disabilities?</td>
<td>All the security/privacy and usability HCI questions How do <strong>users</strong> select graphical passwords? How can we help them choose passwords harder for <strong>attackers</strong> to predict? As the password space increases, what are the impacts on usability factors and predictability of human selection?</td>
</tr>
<tr>
<td>How can we make the password space larger to make the password harder to guess?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How are the stored passwords secured?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can an <strong>attacker</strong> gain knowledge by observing a user entering her password?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Course goals

• Gain an appreciation for the importance of human factors to security and privacy

• Learn about current and important research in the area

• Learn how to conduct user studies targeting security and privacy issues

• Gain tools for critically evaluating research you hear or read about
Course topics

• Quick overviews of security and privacy

• Intro to HCI methods and experimental design
  – How and when to use different qualitative and quantitative study designs
  – Ecological validity and ethics
  – Overview of statistical analysis

• Current/important research on topics of note
  – Passwords, web and mobile privacy, policies and notices, usable encryption, etc.
Topic: Passwords

• Can people make passwords that are easy to remember, yet hard to crack?
Humans have great visual memory… can this fact be leveraged for authentication?
Topic: Biometrics

• Characteristics of the human body can be used to identify or authenticate
  – How can this be done in a user-friendly way?
Topic: Secondary authentication

• Favorite athlete?
• Make of first car?
• Where Barack Obama met his wife?
• Jennifer Lawrence’s mother’s maiden name?
Topic: Censorship, anonymity

• How can we help people to remain anonymous on the Internet? (And should we?)

• How can we help people to evade censorship? (And should we?)

The problem with censorship is
Topic: Usable encryption

- Why don’t people encrypt their email and files?
Topic: SSL and PKIs

- Is there any hope for making certificates and SSL warnings usable?
- Can we teach developers to use SSL correctly?
Topic: Security warnings

- When do we really need them?
- Can we make them more effective?
Topic: Privacy policies and notices

• How do we communicate privacy-critical info?
  – To busy users
  – Despite information overload

Amazon Privacy Policy

<table>
<thead>
<tr>
<th>Types of Information</th>
<th>how we use your information</th>
<th>who we share your information with</th>
</tr>
</thead>
<tbody>
<tr>
<td>contact information</td>
<td>opt in</td>
<td>opt out</td>
</tr>
<tr>
<td>cookies</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>demographic information</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>financial information</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>health information</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>preferences</td>
<td>opt in</td>
<td>opt out</td>
</tr>
<tr>
<td>purchasing information</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>social security number &amp; personal ID</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>your activity on the site</td>
<td>opt out</td>
<td>opt out</td>
</tr>
<tr>
<td>your location</td>
<td>opt out</td>
<td>opt out</td>
</tr>
</tbody>
</table>

Rev. 1/2/10

SoundCloud

- You stay in control of your copyright
- Collected personal data used for limited purposes
- 6 weeks to review changes
- Indemnification
- Personal information

More details

Screenshot from http://www.tosdr.org
Access control, policy configuration

- Who should have access to your files, physical spaces, and online posts?
- How can we make it easier for users to express and enforce their preferences?

Image from http://www.about.com
Topic: Privacy and security at home

• How does the increase in devices and sensors affect privacy dynamics within the home?

• How can these sensors be usably secured?
Topic: Browser privacy & security

• What kind of tracking currently occurs, and what do average people think of it?

• … And why has phishing been so effective?
Topic: HFPS for mobile

- Do people understand where the information on their phone goes?
- …And can someone please make app permissions usable?
Topic: Social networks and privacy

Can people want to share some things widely yet want other things to be private?

A Guide to Facebook’s Privacy Options

- Turn on Secure Browsing to help prevent tracking from reading your Facebook posts or sharing your password.
- Adjust your Security Settings to protect your Facebook account.
- To add protection, turn on Data Protect to make sure Facebook sends a special security code to your phone before you try to log in to Facebook from a new device. If someone steals your Facebook password, they will not be able to log in without this code.
- Click here to configure who can see your future posts, see where you’ve been tagged, and find out what other people can see on your timeline.
- You can change the settings for who can see your future posts here. Be careful! If you change your settings for an individual post, your settings will change for all future posts unless you change the settings again.
- Click here to access privacy settings, app privacy settings, and more. For example, if you’ve previously shared some posts too widely, see the link for “the audience for posts you’ve shared with friends or public.”
- If you like or comment on a post, your comment will be seen by the friends of the person who posted it in a wider audience, depending on that person’s privacy settings.
Topic: Safety-critical devices

• Cars, medical devices, appliances are computers
  – How do we help users protect their privacy and maintain security while still reaping the benefits of these new technologies?
Topic: Economics and behavior

• Can we encourage (nudge) users to make better privacy and security decisions?

• ... And why do Nigerian scammers say they are from Nigeria?

Don't come crying to me when you're hacked.
Topic: Mental models, education

• How do people think about privacy and security?
• How can we educate them?
  – What should they know?

Image from http://www.quickmeme.com
Course website

- [https://sites.umiacs.umd.edu/mmazurek/courses/818d-s16/](https://sites.umiacs.umd.edu/mmazurek/courses/818d-s16/)
- Assignments posted and submitted via ELMS
- Discussions: ELMS or Piazza?
Your grade

- Project: 40%
- Homework: 15%
- Final exam: 15%
- Class presentation: 10%
- Reading reports: 10%
- Class participation: 10%
Reading and reports

• Usually 2 required readings per class
  – Several additional optional readings
  – Complete **BEFORE** class!

• 20 reports per student (10%)
  – Brief summary (3-5 sentences) and **comment** for each required reading, one optional reading
  – Due at start of class

• If you don’t do the reading, we can’t discuss
Class participation (10%)

• Contribute to in-class discussions, activities
  – Do the reading!
  – Go to relevant seminars and tell us about them

• Contribute to class discussion board
  – ELMS or Piazza?
  – Share interesting privacy/security news
  – Ask questions and spark discussion
  – Answer questions for other students
Class presentation (10%)

• Lead class for 45+ min on assigned day
  – Bid for preferred dates
• DON’T: just present reading summaries
• DO: required and optional reading
• DO: demo, discussion, activity, additional sources, etc.
Homework (15%)

• Exercise skills for designing/critiquing experiments and tools, analyzing data
  – Sketch a tool
  – Evaluate a tool
  – Conduct a mini user study
  – Propose possible studies
  – Analyze sample data
  – Etc.

• Five total

• HW1 due next Tuesday—Thursday
Final exam

• Take-home, during the last week of class
• Much like a longer homework
Project (40%)

• Design, conduct, and analyze a user study related to security or privacy
  – Pitch projects in class
  – Result in groups of 3-5

• Deliverables: project proposal, IRB application, progress report, final paper and talk
  – Workshop-quality paper

• Preferred goals: Submit a poster to SOUPS 2016, and/or a paper to NDSS 2017 or CHI 2017
Example projects (mostly CMU)

• An inconvenient trust: User attitudes toward key-directory encryption systems (submitting to SOUPS 2016)

• The post that wasn’t: Exploring self-censorship on Facebook (CSCW 2013)

• Exploring reactive access control (CHI 2011)

• How does your password meter measure up? The effect of strength meters on password creation (USENIX Sec 2012)

• Passwords gone mobile (CHI 2016)

• … and others!
Academic integrity

• Homework assignments and exam are INDIVIDUAL unless otherwise noted
  – Don’t look at other students’ assignments

• Zero-tolerance policy for plagiarism
  – Includes reading reports!
  – Even one sentence is too much. Rewrite in your words.
  – When in doubt, ASK BEFORE YOU SUBMIT

• Review university policies as needed
Other miscellaneous

• I expect you in class
  – Foreseeable family obligations, holidays, conferences, etc: send me email in the next week
  – Unforeseeable: let me know

• Consider joining:
  – MC2-discuss@umiacs
  – MC2-announce@umiacs
  – hcil@cs
The human threat

• Malicious humans
• Humans who don’t know what to do
• Unmotivated humans
• Humans with human limitations
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**
Are you capable of remembering a unique strong password for every account you have?
Key challenges

• Security is a secondary task
• Security concepts are hard
• Human capabilities are limited
• Habituation
  – The “crying wolf” problem
• Misaligned priorities
Keep the bad guys out
Don’t lock me out!
Key challenges

• Security is a secondary task
• Security concepts are hard
• Human capabilities are limited
• Habituation
• Misaligned priorities
• Active adversaries
  – Unlike ordinary UX
What is Twitter?

Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick, frequent answers to one simple question: What are you doing?
Case study #1:

GREY AND USER BUY-IN
Grey: Smartphone-enabled doors

- Access control system for doors in the CMU CyLab offices
- Based on formal proofs of access
  - Allows users to grant access to others remotely
- Year-long interview study
  - 29 users x 12 accesses per week


Users complained about speed

• Videotaped a door to understand how Grey is different from keys
Average access times

Grey is not noticeably slower than keys!

Getting keys → Stop in front of door → Door opened → Door Closed

- Getting keys: 3.6 sec, σ = 3.1
- Stop in front of door: 5.4 sec, σ = 3.1
- Door opened: 5.7 sec, σ = 3.6
- Door Closed: Total 14.7 sec, σ = 5.6

Getting phone → Stop in front of door → Door opened → Door Closed

- Getting phone: 8.4 sec, σ = 2.8
- Stop in front of door: 2.9 sec, σ = 1.5
- Door opened: 3.8 sec, σ = 1.1
- Door Closed: Total 15.1 sec, σ = 3.9

Grey is not noticeably slower than keys!
“I find myself standing outside and everybody inside is looking at me standing outside while I am trying to futz with my phone and open the stupid door.”

**Takeaway: Misaligned priorities**
Case Study #2

PASSWORD EXPIRATION AND USER BEHAVIOR
Does password expiration improve security in practice?

• **Observation**
  - Users often respond to password expiration by transforming their previous passwords in small ways [Adams & Sasse 99 … we’ll talk about this later]

• **Conjecture**
  - Attackers can exploit the similarity of passwords in the same account to predict the future password based on the old ones

[Zhang et. al, CCS 2010]
Empirical analysis

• UNC “Onyen” logins
  – Broadly used by campus and hospital personnel
  – Password change required every 3 months
  – No repetition within 1 year

• 51141 unsalted hashes, 10374 defunct accounts
  – 4 to 15 hashes per account in temporal order

• Cracked ~8k accounts, 8 months, standard tools

• Experimental set: 7752 accounts
  – At least one cracked password, NOT the last one
Transform Trees

- Approximation algorithm for optimal tree searching
## Location Independent Transforms

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capitalization</td>
<td>tarheels#1 → tArheels#1</td>
</tr>
<tr>
<td>Deletion</td>
<td>tarheels#1 → tarheels1</td>
</tr>
<tr>
<td>Duplication</td>
<td>tarheels#1 → tarheels11</td>
</tr>
<tr>
<td>Substitution</td>
<td>tarheels#1 → tarheels#2</td>
</tr>
<tr>
<td>Insertion</td>
<td>tarheels#1 → tarheels12</td>
</tr>
<tr>
<td>Leet Transform</td>
<td>tarheels#1 → t@rheels#1</td>
</tr>
<tr>
<td>Block Move</td>
<td>tarheels#1 → #tarheels1</td>
</tr>
<tr>
<td>Keyboard Transform</td>
<td>tarheels#1 → tarheels#!</td>
</tr>
</tbody>
</table>
Evaluation

• Pick a known plaintext, non-last password (OLD)
• Pick any later password (NEW)
• Attempt to crack NEW with transform tree rooted at OLD
Results: Offline Attack

Takeaways: Memory limitations matter
Convenience always wins
Understanding the human

• Who wants to practice good security but doesn’t know how

• Who is indifferent to security but will comply
  – If it’s easy
  – If it’s the default
  – If it doesn’t interfere with the primary task
Human-in-the-loop framework

• Based on Communication-Human Information Processing Model (C-HIP) from Warnings Science

• Models human interaction with secure systems

• Can help identify (non-malicious) human threats

Human-in-the-loop framework

Communication Impediments
- Environmental Stimuli
- Interference

Communication

Human Receiver

Personal Variables
- Demographics and Personal Characteristics
- Knowledge & Experience

Communication Delivery
- Attention Switch
- Attention Maintenance

Communication Processing
- Comprehension
- Knowledge Acquisition

Application
- Knowledge Retention
- Knowledge Transfer

Intentions
- Attitudes and Beliefs
- Motivation

Capabilities

Behavior
Human threat identification and mitigation process

- **Task Identification**: Identify points where the system relies on humans to perform security-critical functions.
- **Task Automation**: Find ways to partially or fully automate some of these tasks.
- **Failure Identification**: Identify potential failure modes for remaining tasks.
- **Human-in-the-loop Framework**: User Studies
- **Failure Mitigation**: Find ways to prevent these failures.
Human-in-the-loop framework

Communication

Communication Impediments
- Environmental Stimuli
- Interference

Human Receiver

Personal Variables
- Demographics and Personal Characteristics
- Knowledge & Experience

Intentions
- Attitudes and Beliefs
- Motivation

Capabilities

Communication Delivery
- Attention Switch
- Attention Maintenance

Communication Processing
- Comprehension
- Knowledge Acquisition

Application
- Knowledge Retention
- Knowledge Transfer

Behavior
浴衣・スリッパのままで、客室フロア（廊下）以外へ外出になることは、非常時を除き、ご遠慮ください。
Internet Explorer cookie flag
Human threat identification and mitigation process

Task Identification
Identify points where system relies on humans to perform security-critical functions

Task Automation
Find ways to partially or fully automate some of these tasks

Failure Identification
Identify potential failure modes for remaining tasks

Failure Mitigation
Find ways to prevent these failures

Human-in-the-loop Framework
User Studies
<table>
<thead>
<tr>
<th>Component</th>
<th>Questions to ask</th>
<th>Factors to consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>What type of communication is it (warning, notice, status indicator, policy, training)? Is communication active or passive? Is this the best type of communication for this situation?</td>
<td>Severity of hazard, frequency with which hazard is encountered, extent to which hazard is encountered, action is necessary to avoid hazard</td>
</tr>
<tr>
<td>Communication</td>
<td></td>
<td>Other related and unrelated communications, user’s primary task, ambient light, noise</td>
</tr>
<tr>
<td>Communication</td>
<td>Environmental Stimuli What other environmental stimuli are likely to be present?</td>
<td>Malicious attackers, technology failures, environmental stimuli that obscure the communication</td>
</tr>
<tr>
<td>Communication</td>
<td>Interference Will anything interfere with the communication being delivered as intended?</td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Personal Variables Demographics and personal characteristics Who are the users? What do their personal characteristics suggest about how they are likely to behave?</td>
<td>Age, gender, culture, education, occupation, disabilities</td>
</tr>
<tr>
<td>Communication</td>
<td>Knowledge and experience What relevant knowledge or experience do the users or recipients have?</td>
<td>Education, occupation, prior experience</td>
</tr>
<tr>
<td>Communication</td>
<td>Intentions Attitudes and beliefs Do users believe the communication is accurate? Do they believe they should pay attention to it? Do they have a positive attitude about it?</td>
<td>Reliability, conflicting goals, distraction from primary task, risk perception, self-efficacy, response efficacy</td>
</tr>
<tr>
<td>Communication</td>
<td>Motivation Are users motivated to take the appropriate action? Are they motivated to do it carefully or properly?</td>
<td>Conflicting goals, distraction from primary task, convenience, risk perception, consequences, incentives/disincentives</td>
</tr>
<tr>
<td>Communication</td>
<td>Knowledge and characteristics</td>
<td>Knowledge, education, experience, ability</td>
</tr>
<tr>
<td>Capabilities</td>
<td>Communication delivery</td>
<td>Communication processing</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td>Attention switch</td>
<td>Attention maintenance</td>
</tr>
<tr>
<td></td>
<td>Do users notice the communication? Are they aware of rules, procedures, or training messages?</td>
<td>Do users pay attention to the communication long enough to process it? Do they read, watch, or listen to it fully?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knowledge, cognitive or physical skills, memorability, required software or devices</td>
<td>Environmental stimuli, interference, format, font size, length, delivery channel, habituation</td>
</tr>
<tr>
<td></td>
<td>Environmental stimuli, format, font size, length, delivery channel, habituation</td>
<td>Symbols, vocabulary and sentence structure, conceptual complexity, personal variables</td>
</tr>
<tr>
<td></td>
<td>Exposure or training time, involvement during training, personal characteristics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Involvement during training, similarity of training, personal characteristics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type of behavior, ability of people to act randomly in this context, usefulness of prediction to attacker</td>
<td></td>
</tr>
</tbody>
</table>
Users are not the enemy

• Adams and Sasse, CACM 1999

• “These observations cannot be disputed, but the conclusion that this behavior occurs because users are inherently careless — and therefore insecure — needs to be challenged.”

• Study methods:
  – Online survey, primarily from organization A
  – Interviews at organizations A and B
  – Grounded theory
Results (Highlights)

• Circumventing rules to get work done
  – Shared passwords, predictable choices
• Multiple passwords lead to problems
• Limited knowledge of what pwds are secure
  – Limited knowledge of threats
Discussion questions

• This paper is “classic” (from 1999). What do you think might be different today? What questions would you add or change?

• Are these participants representative (of what)?
  – What other groups could you ask? How might the results be different?
Discussion questions

• “Users identified certain systems as worthy of secure password practices, while others were perceived as ‘not important enough.’”
  – How do you motivate users?
  – How do you treat users as partners?
  – What about when this behavior is rational/correct?

• List of proposed solutions
  – Do you think these would work? Why / why not?
  – Other suggestions?
(One) Hierarchy of solutions

• 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
Automation considered harmful?

Problems:

• Insufficient flexibility
• Imposition of values
• Impact on user experience
  – Especially in failure cases

• Examples from your home domain?
Considerations for automating

• Accuracy
• Stakeholder values
• Information overload?
• Implicit instead?
• Keep human informed?
• Fail gracefully?

• Do you agree with all of these?
• Are there others we should add?
Suggested research directions

Suggested directions:

• Exposing system behavior

• Causality and contextualization
  – Identify root causes
  – Moving system -> application

• Social identity and decisionmaking
  – People rather than devices
  – Multiple, flexible social identities
Discussion questions

• This one is from 2007. How do you think these issues have evolved in the meantime?

• Problems/solutions in your home domain
  – How do they fit into this framework?

• Problems/challenges in the suggested directions?