Why Usability Can’t Be Just Skin Deep

Lujo Bauer
18-732
Spring 2015
Usability & Secure Software Systems

- Software systems interact with humans
  - Administrators, end users

- Design goals of a system almost always (perhaps implicitly) include humans as part of that system
  - Features are no good if people can’t use them
  - A system isn’t secure if users always make mistakes

- For practical definitions of security, a system cannot be “secure” unless it is usable
“Usability” often seen as the last phase in system design

Thesis:

*Creating usable systems often requires not just the help of usability experts, but that the system architects are usability experts*
This Lecture: Three Examples

- Ex 1: subtle design choices can have an unpredicted impact on usability
- Ex 2: fundamental design choices can limit/create options for improving usability
- Ex 3: design needs to be informed by understanding of users’ requirements
Ex 1: Access-control Policy Semantics
Policy Interface

Problems with List-of-rules Interfaces

- **Scale**
  - Only one rule at a time is visible

- **Groups**
  - Group membership information is not visible

- **Rule conflicts**
  - When rules interact, it isn’t clear what the outcome will be
Policy Interface

Jana Task – Common Error

Four-part Harmony.doc Properties

Group or user names:
- jana (CARNEGIE-7CF6DD\jana)
- Theory 101 Instructors (CARNEGIE-7CF6DD\Theory 101 I)
- Theory 101 Students 2007 (CARNEGIE-7CF6DD\Theory 101 T)
- Theory 101 TAs 2006 (CARNEGIE-7CF6DD\Theory 101 T)
- Theory 101 TAs 2007 (CARNEGIE-7CF6DD\Theory 101 T)

Permissions for jana
- Full Control: Allow, Deny
- Modify: Allow, Deny
- Read & Execute: Allow, Deny
- Read: Allow
- Write: Allow
- Special Permissions: Allow, Deny

For special permissions or for advanced settings, click Advanced.

OK | Cancel | Apply
Policy Interface

Learning Jana’s Effective Permissions

1. Click “Advanced”

2. Click “Effective Permissions”

3. Select Jana

4. View Jana’s Effective Permissions
Bring up Computer Management interface

1. Click on "Users"
2. Double-click Jana
3. Click "Member Of"
4. Read Jana’s group membership

TAs 2006
TAs 2007
Click on TAs 2006

Read permissions for TAs 2006

Click on TAs 2007

Read permissions for TAs 2007
Policy Interface

Changing Jana’s Groups’ Permissions

14

Click on TAs 2006

15

Change permissions for TAs 2006
Policy Interface

Checking Work

16. Click “Advanced”

17. Click “Effective Permissions”

18. Select Jana

19. View Jana’s Effective Permissions
A New Interface: The Expandable Grid
[Reeder, Bauer, Cranor, Reiter, Vaniea CHI 2008, CHI 2011]

- Shows effective policy instead of policy rules
- Shows both user and file hierarchies (groups)
- Shows entire policy on one screen
## Study Results: Grid vs Windows

<table>
<thead>
<tr>
<th>Task type</th>
<th>Grid</th>
<th>Windows</th>
<th>Small-size</th>
<th>Large-size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Accuracy</td>
<td>Time</td>
</tr>
<tr>
<td>View simple</td>
<td></td>
<td></td>
<td>89%</td>
<td>29s</td>
</tr>
<tr>
<td>View complex</td>
<td>94%</td>
<td>64s</td>
<td>17%</td>
<td>35s</td>
</tr>
<tr>
<td>Change simple</td>
<td></td>
<td>52s</td>
<td>94%</td>
<td>30s</td>
</tr>
<tr>
<td>Change complex</td>
<td>61%</td>
<td>70s</td>
<td>0%</td>
<td>100%</td>
</tr>
<tr>
<td>Compare groups</td>
<td></td>
<td>103s</td>
<td>89%</td>
<td>39s</td>
</tr>
<tr>
<td>Conflict simple</td>
<td>67%</td>
<td>55s</td>
<td>61%</td>
<td>103s</td>
</tr>
<tr>
<td>Conflict complex</td>
<td></td>
<td>103s</td>
<td>89%</td>
<td>70s</td>
</tr>
<tr>
<td>Memogate simulation</td>
<td>100%</td>
<td>118s</td>
<td>94%</td>
<td>20s</td>
</tr>
<tr>
<td>Precedence rule test</td>
<td>89%</td>
<td>42s</td>
<td>94%</td>
<td>42s</td>
</tr>
</tbody>
</table>
Study Results: Conflict Resolution

- But... We changed conflict-resolution method to recency-takes-precedence
- Were the effects of our original study due to the new visualization idea, the new conflict-resolution method, or both?
- We ran another study to find out
Semantics Study

- Laboratory study
- 3 conditions:
  - Expandable Grid with specificity semantics
  - Expandable Grid with Windows semantics
  - Native Windows file permissions interface
- 54 participants, 18 per condition, novice policy authors
- 10 minutes training for all conditions
- 12 tasks
Charles Task

- Charles has just graduated, but is going to come back to sing in the choir with his friends
- Add Charles to the Alumni group, but make sure he can still read the same files in the Choir 1\Lyrics folder that his good friend Carl can read
1. Does semantics make a difference?  YES
2. Does specificity help resolve rule conflicts?  YES
3. Is specificity semantics always better than Windows?  NO
Example 1 Summary

- Changing semantics has effect on usability, regardless of interface
Ex 2: Policy Configuration in Grey

- Smartphone-based, end-user-driven access-control system for physical and virtual resources
- Deployed in CMU’s Collaborative Innovation Center
  - Approximately 40 Grey-capable doors and 60+ users at the moment
Grey: An Example Scenario

- Lujo’s students are allowed in 2121
- Faculty are allowed in 2121
- At CMU, Lujo’s secretary speaks on behalf of Lujo

Lujo must authorize access

I need to grade the midterms for Lujo’s class

Lujo’s Office, 2121
Grey: An Example Scenario

1. Hi, Please open 2121

2. Prove Lujo says open 2121

3. Prove Scott says open 2121 → Lujo says open 2121

4. Proof of Scott says open 2121 → Lujo says open 2121

5. Proof of Lujo says open 2121

Provable if Lujo says:
- Open 2121
- Scott speaks for Lujo
- Scott is a student
- Scott is faculty
- ...

This is Lujo’s belief. I’ll ask Lujo for help.

Generate credential stating Scott’s desire to open 2121
Can We Make Configuration Easier?

- Setting up policies takes effort
- Incorrectly set up policies can wrongly allow or deny access

- How to help users easily set up correct policies?
Can We Make Configuration Easier? 
[Bauer, Garriss, Reiter SACMAT 2008, ...]

- Setting up policies takes effort
- Incorrectly set up policies can wrongly allow or deny access
- How to help users easily set up correct policies?
- Mechanism involves two steps:
  - Identifying intended policy and misconfigurations in the implemented policy
  - Resolving misconfigurations by augmenting the implemented policy
- “Misconfiguration” refers to authority that is intended to exist but has not been given
Identifying Misconfigurations

- **Observation:** access-control policy exhibits patterns
  - Inconsistencies in these patterns can indicate misconfigurations
  - These patterns are observable from access-control logs
  - Need centralized collection of logs to analyze

- **Use Association Rule Mining** [Agrawal and Srikant ’94]
  - Input: series of records characterized by a fixed number of attributes
  - Output: rules (or statistical patterns)

- **Use rules to identify anomalies**
### Identifying Misconfigurations

<table>
<thead>
<tr>
<th></th>
<th>ResA</th>
<th>ResB</th>
<th>ResC</th>
<th>ResD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>T</td>
<td>-</td>
<td>T</td>
<td>-</td>
</tr>
<tr>
<td>Bob</td>
<td>T</td>
<td>T</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Charlie</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>-</td>
</tr>
<tr>
<td>David</td>
<td>T</td>
<td>-</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

**Rule:** ResA → ResC

**Resources**

**Users**

**Potential Misconfiguration (a.k.a., a prediction)**
Dataset

- Log of 10,911 accesses drawn from Grey deployment
- Spans 16 months
- Contains accesses by 25 users to 29 resources
Identification Simulation

Chronological Access History

Intended Policy Matrix

Prediction correctly identifies a misconfiguration

(A \rightarrow C)
Accuracy/Coverage Tradeoff

Good compromise:
~70% accuracy
~55% coverage:
0.3 < minconf < 0.5
High-Latency Accesses

44% reduction in high-latency accesses
Total User Interaction Time
(across all users over 16 months)

All time spent resolving misconfigurations proactively is offset by time-of-access savings
Ex 2 Summary

- Machine learning can help with policy configuration
- Needs centralized collection of access logs
  - Helps if access logs explain why access was granted
Ex 3: Securing the Digital Home
The Home Has Gone Digital... Can We Handle It?

- **Plethora of networked consumer electronics**
  - Exciting new capabilities for users
  - But, who handles security and reliability?

- **Goal: usable security for the digital home**
  - Enable users to effectively specify and understand policies
  - Enable users to use and trust mechanisms
User Study: Exploring Home Access Control

[Mazurek, Arsenault, Bresee, Gupta, Ion, Johns, Lee, Liang, Olsen, Salmon, Shay, Vaniea, Bauer, Cranor, Ganger, Reiter CHI 2010]

- Technical researchers usually poor judges of users
  - Tend to design things that work well for themselves

- Home security will only work if it works for home users
  - “Normal people” who don’t do technology 24/7/365

- Seek to understand attitudes, needs, and current practices

- Explore access-control dimensions:
  - Current access-control practices: digital, paper
  - Person, location, device, time of day
  - Logs, reactive delegation
  - etc...
Designing a User Study

- In-situ, semi-structured interviews
  - Recruitment via Craigslist, fliers
  - Limited to non-programmer households

- Interviewed 33 users in 15 households
  - Families, couples, roommates
  - Ages 8 to 59

- Recorded and transcribed over 30 hours of interviews
House Maps Guided Interviews
Interview Structure and Question Style

- For each dimension, start with a specific scenario
- Example: *Imagine that a friend is in your house when you are not. What kinds of files would you (not) want them to be able to [view, change]?
  - Would it be different if you were also in the [house, room]?

- Extend to discuss that dimension in general
- Likert scale to rate concern over certain policy violations:
  - 1 = don’t care; 5 = devastating
Finding: Current Methods Aren’t Working

- People do worry about sensitive data
  - Many potential breaches rated as “devastating”
  - Almost all worry about file security sometimes
  - Several have suffered actual breaches

- Access-control mechanisms varied and (often) ad hoc
  - Encryption, user accounts (some people)
  - Hide sensitive files in the file system
    “If you name something ‘8F2R349,’ who’s going to look at that?”
  - Delete sensitive data so no one can see it
    “If I didn’t want everyone to see them, I just had them for a little while and then I just deleted them.”
Finding: Policy Needs Are Complex

- **Fine-grained divisions of people and files**
  - Public, private aren’t enough
  - More than friends, family, colleagues, strangers

- **Dimensions beyond person**
  - Presence resonates for most
    - “If you have your mother in the room, you are not going to do anything bad. But if your mom is outside the room you can sneak.”
    - Also gives a chance to explain
  - Location matters for many
    - People in my home are trusted
  - Read-only is needed but not sufficient
  - Device, time of day not as popular
Finding: Policy Needs Are Complex

- Variation across participants
  - Finding reasonable defaults is difficult
  - Sharing-oriented vs. restriction-oriented
    “Basically, it’s my stuff; if I want you to have it, I’ll give it to you.”
    “I don’t really have private files.... There’s nothing that I am hiding from anybody.”
  - Most have one “most trusted” person
    • But definition of “most trusted” varies widely
  - What is most/least private?
Twenty-something middle school Spanish teacher:

“Wouldn’t want my boss to see me in my swimsuit.... I just wouldn’t like him to see it.”
Twenty-something paralegal and law student would let her boss see photo of her drunk, dancing on a table: “he’s seen me do it in person before.”
Finding: A-priori Policy Isn’t Good Enough

- People like to be asked permission
  - Positive response to reactive policy creation
    “I’m very willing to be open with people, I think I’d just like the courtesy of someone asking me.”
  - Setting a-priori policy doesn’t convey control like being present and/or explicitly granting permission

- People want to know both who is accessing files and why

- People want to review accesses and revise policy
Finding: Mental Models $\neq$ System Realities

- Mismatch between current systems and mental models may lead users astray
  - Hiding files in the file system
  - Preventing policy violations with presence
    “If anything were to happen, ... I’m right there to say, ‘OK, what just happened?’ So I’m not as worried.”
  - Physical device boundaries: Anyone using my device can see everything; no one not touching my device can see anything
Design Guidelines Exposed by User Study

- Allow fine-grained control
- Plan for lending devices
- Include reactive policy creation and usable logs
- Reduce or eliminate up-front complexity
- Acknowledge social conventions
- Support iterative policy specification
- Account for users’ mental models
Ex 3 Summary

- User study prior to designing a system can lead to unexpected findings
  - Features users want
  - Ways in which system may be used
  - Users’ understanding of concepts relevant to system
Why Usability Can’t Be Just Skin Deep

Thesis:

Creating usable systems often requires not just the help of usability experts, but that the system architects are usability experts

- Decisions that affect usability need to be made at the outset
- Certain system designs may be more amenable to advancing usability than others
  - Features, architecture, APIs
- User studies before designing system can reveal unexpected system requirements
  - Features, understanding of relevant concepts
Next

- Thu 4/16: No class! -- Carnival
- Tue 4/21: Security-typed languages
- Thu 4/23: Typed assembly language