03- Reasoning about the Human in the Loop

Lorrie Cranor, Blase Ur, and Rich Shay

January 20, 2015

05-436 / 05-836 / 08-534 / 08-734

Usable Privacy and Security
Today!

• Human in the Loop Framework
• Everyday usability
• Privacy illustrated
The Human in the Loop
The human threat

- Malicious humans
- Clueless humans
- Unmotivated humans
- Humans constrained by human limitations
Are you capable of remembering a unique strong password for every account you have?
Security is a secondary task
Concerns may not be aligned

Keep the bad guys out

Don’t lock me out!

Security Expert

User
Grey

- Smartphone based access-control system
- Used to open doors in the Carnegie Mellon CIC building
- Allows users to grant access to their doors remotely


Data collection

- Year long interview study
- Recorded 30 hours of interviews with Grey users
- System was actively used: 29 users x 12 accesses per week
Users complained about speed

• Users said Grey was slow
• But Grey was as fast as keys
• Videotaped a door to better understand how doors are opened differently with Grey and keys
Average access times

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
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
“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.”
Nobody wants to have to reboot their door
Unanticipated uses can bolster acceptance
Convenience always wins
How can we make secure systems more usable?

• 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
Try to better understand humans in the loop

• Do they know they are supposed to be doing something?
• Do they understand what they are supposed to do?
• Do they know how to do it?
• Are they motivated to do it?
• Are they capable of doing it?
• Will they actually do it?
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 human threats

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

Communication Impediments
- Environmental Stimuli
- Interference

Communication

Behavior

Human-in-the-loop framework
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**:
  - Human-in-the-loop Framework
  - User Studies
  - Identify potential failure modes for remaining tasks.

- **Failure Mitigation**: Find ways to prevent these failures.

Flowchart illustration:

1. Task Identification
2. Task Automation
3. Failure Identification
4. Failure Mitigation

User Studies

Identify points where system relies on humans to perform security-critical functions.
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
Internet Explorer cookie flag
Privacy policy *matches* user’s privacy preferences

Privacy policy *does not match* user’s privacy preferences
WARNING
AUTOS ONLY
NO PEDESTRIANS
NO MOTORCYCLES
NO BICYCLES

KEEP AWAY FROM GATE ARM
MOVING GATE ARM CAN CAUSE
SERIOUS INJURY OR VEHICLE DAMAGE

Moving Gate Can Cause Serious Injury or Death
浴衣・スリッパのままで、客室フロア（廊下）以外へお出になることは、非常時を除き、ご遠慮ください。
Warnings
Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegaforse.

Image courtesy of Johnathan Nightingale
What to do about hazards?
Best solution: remove hazard
Next best: guard against hazard
If all else fails: warn
CAUTION
CAUTION UNEVEN SURFACES
Human threat mitigation for warnings

Determine whether task I am trying to complete is sufficiently risky that I should stop.
Automate and change tasks to reduce need for user involvement

Might be dangerous

User must decide

Use automated analysis to determine probability of danger
Support user decision

- **High probability of danger**: Block
- **Might be dangerous**: User must decide
- **Very low probability of danger**: Don’t bother user

Improve warnings

Help user decide by asking question user is qualified to answer
Bad question

Your web browser thinks this is a phishing web site. Do you want to go there anyway?

Don’t go there    Go there anyway

I don’t know what a phishing site is.

I really want to go to this site.

Of course I will go there anyway!
Better question

You are trying to go to evilsite.com. Do you really want to go there or would you rather go to yourbank.com?

Go to yourbank.com  Go to evilsite.com

Of course I want to go to yourbank.com!
Everyday usability
Unione Commercio Turismo e Attività di Servizio

VIETATO FUMARE

RAUCHEN VERBOTEN

NO SMOKING
Please leave me on.
I will turn the light and fan off automatically after 4 minutes of detecting no movement.

I will turn on automatically when someone walks in.
Please press the ON button.
Please note that this facility is not equipped with an automatic flushing system. Please flush prior to leaving the stall.

Thank you for your cooperation,

CBRE
CB Richard Ellis
If toilet does not flush automatically before you exit the stall, please press button on the side of the cylinder to flush.
The Vancouver Convention Centre is committed to sustainability and uses recycled non-potable water from its Water Treatment Facility to flush toilets and urinals. This water is not intended for consumption.
This bathtub has been treated with snash 2000 anti-slip substance for your safety

אמונתיוזעברה cellpadding 2000
לmiştir החלקה בביתוחך האישיות

SNASH int Markating
 Snackbar שיווק בינלאומי ברעם
Tel.912-3-5748483
Please make an effort to keep this bathroom clean for everyone who uses it. No trash on the floor, clean up after yourself and please be neat.

Please clean the **user interface** when your application is completed.

Thank you.
IMAGES OF PRIVACY

What does privacy mean to you? We asked people to draw what privacy means to them. We went into schools to ask children of different ages, and we asked adults across the United States to contribute their images of privacy. Now we’re asking people around the world to add to our collection. Explore the drawings here:

abstract  ads  age 20-29  age 30-39  age 40-49  age 50-59  age 60-69  age 90-99  alone  alone/private space  anonymous  away from family  bank statement  basement  bathing  bathroom  bedroom  big brother  blanket  box  brain  browser