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

Carnegie Mellon University
CyLab

institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today!

- Human in the Loop Framework
- Everyday usability
- Privacy illustrated

The Human in the Loop

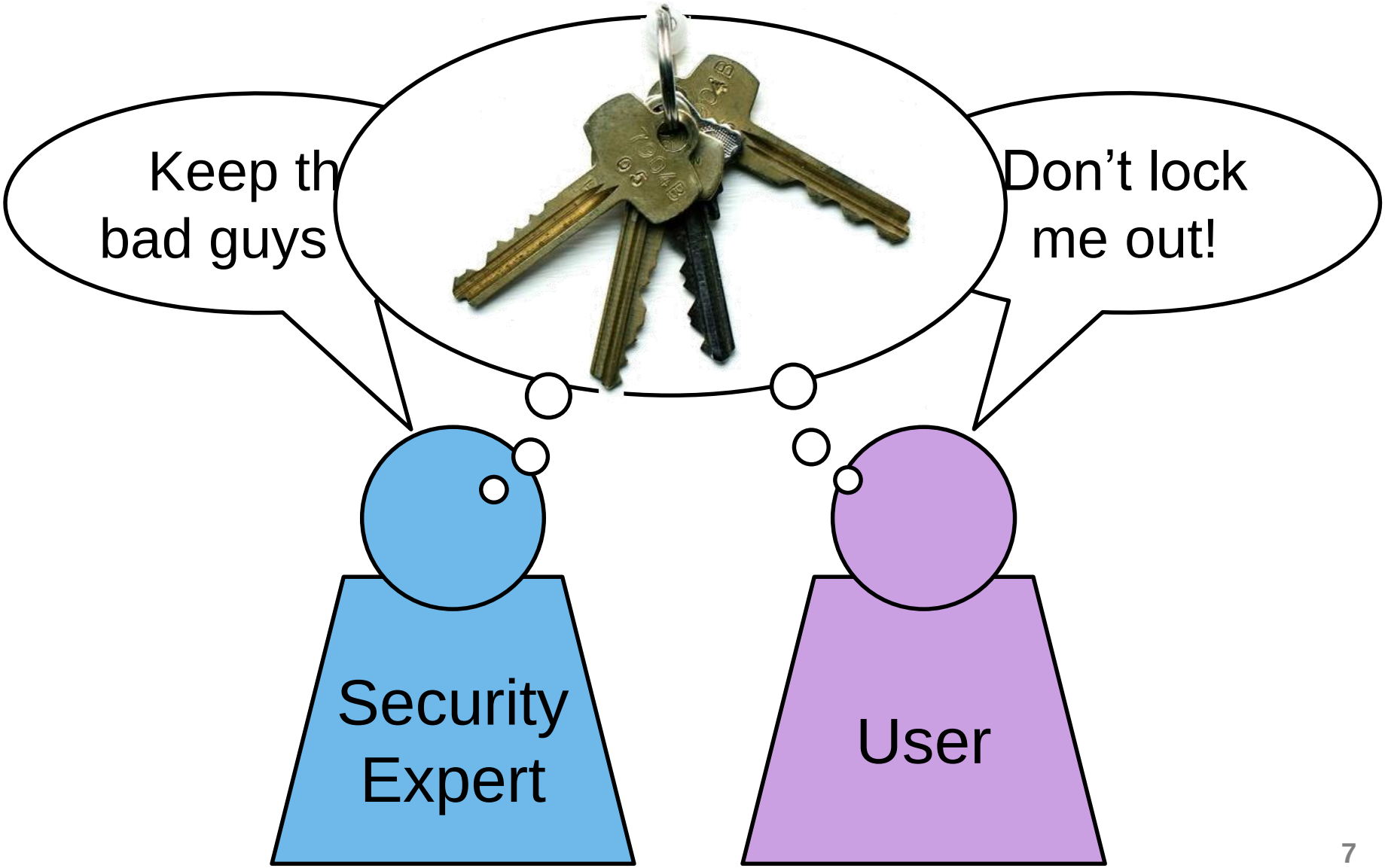
The human threat

- 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



Grey

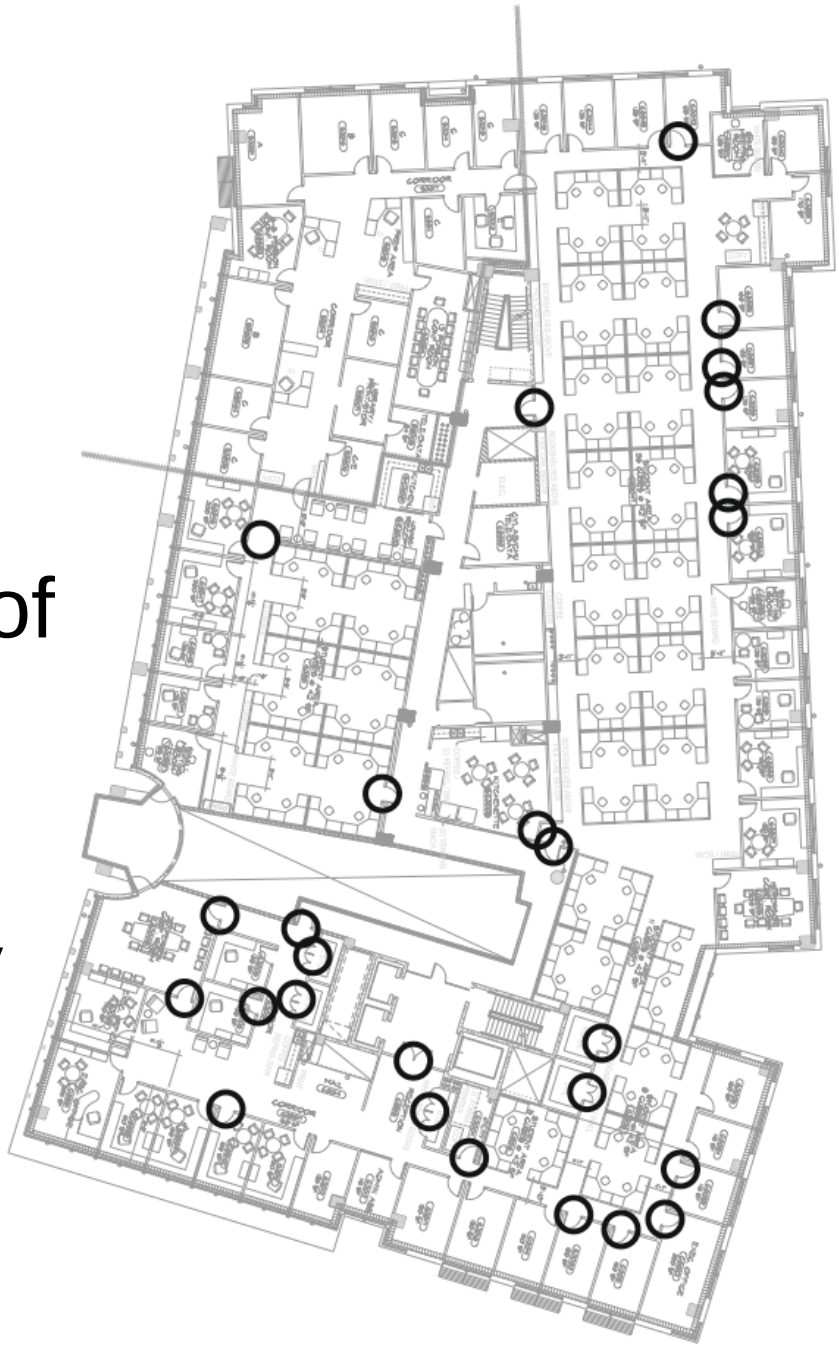
- Smartphone based access-control system
- Used to open doors in the Carnegie Mellon CIC building
- Allows users to grant access to their doors remotely

L. Bauer, L.F. Cranor, R.W. Reeder, M.K. Reiter, and K. Vaniea. **A User Study of Policy Creation in a Flexible Access-Control System.** CHI 2008. http://www.robreeder.com/pubs/greyCHI2008.pdf

L. Bauer, L. F. Cranor, M. K. Reiter, and K. Vaniea. **Lessons Learned from the Deployment of a Smartphone-Based Access-Control System.** SOUPS 2007. http://cups.cs.cmu.edu/soups/2007/proceedings/p64_bauer.pdf

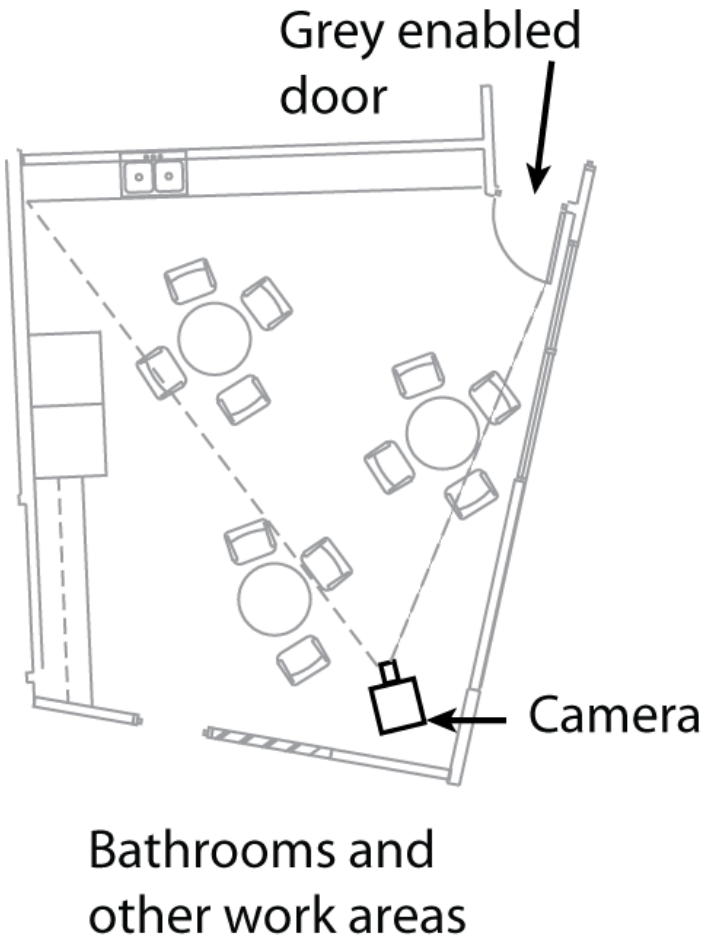
Data collection

- 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

3.6 sec
σ = 3.1

5.4 sec
σ = 3.1

5.7 sec
σ = 3.6

Getting keys

Stop in front of door

Door opened

Door Closed

Total 14.7 sec

σ = 5.6

8.4 sec
σ = 2.8

2.9 sec
σ = 1.5

3.8 sec
σ = 1.1

Getting phone

Stop in front of door

Door opened

Door Closed

Total 15.1 sec

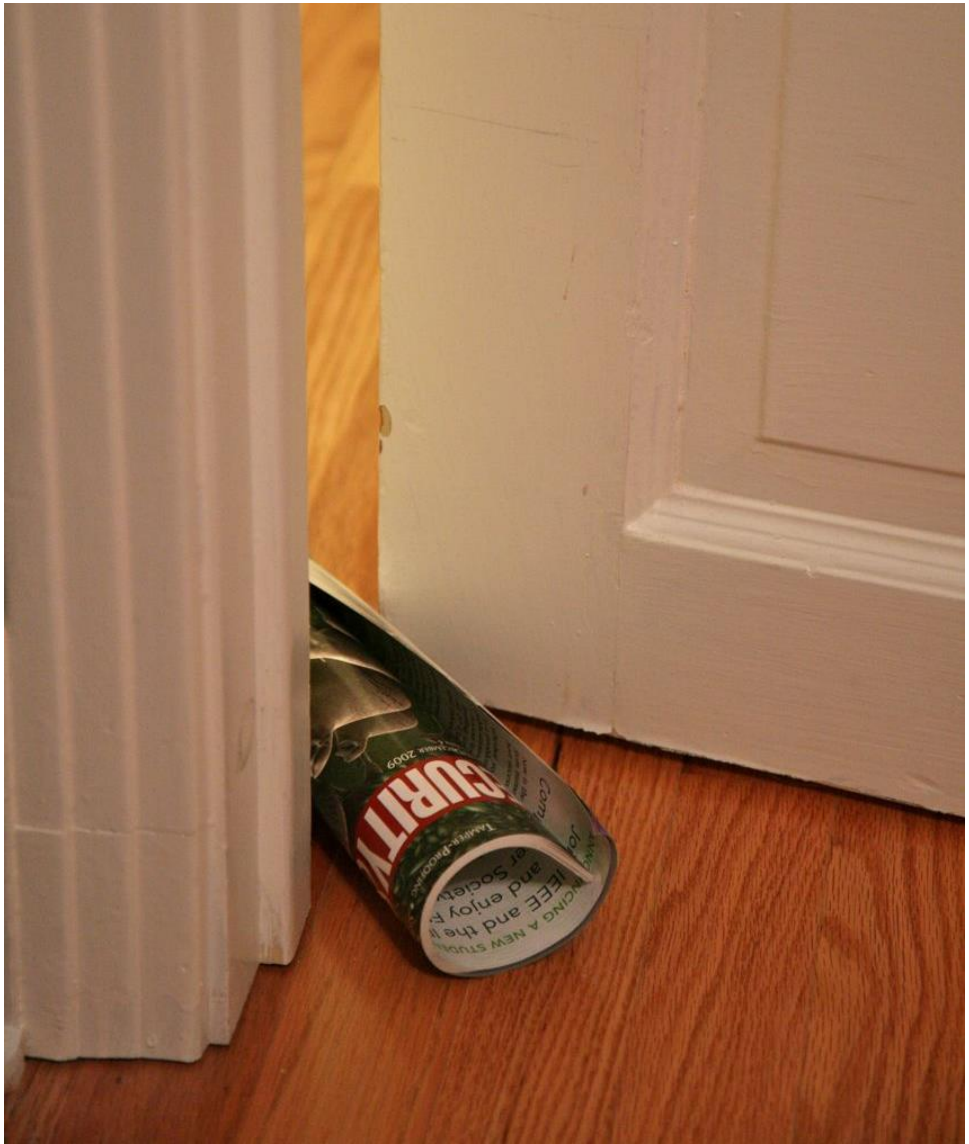
σ = 3.9

“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

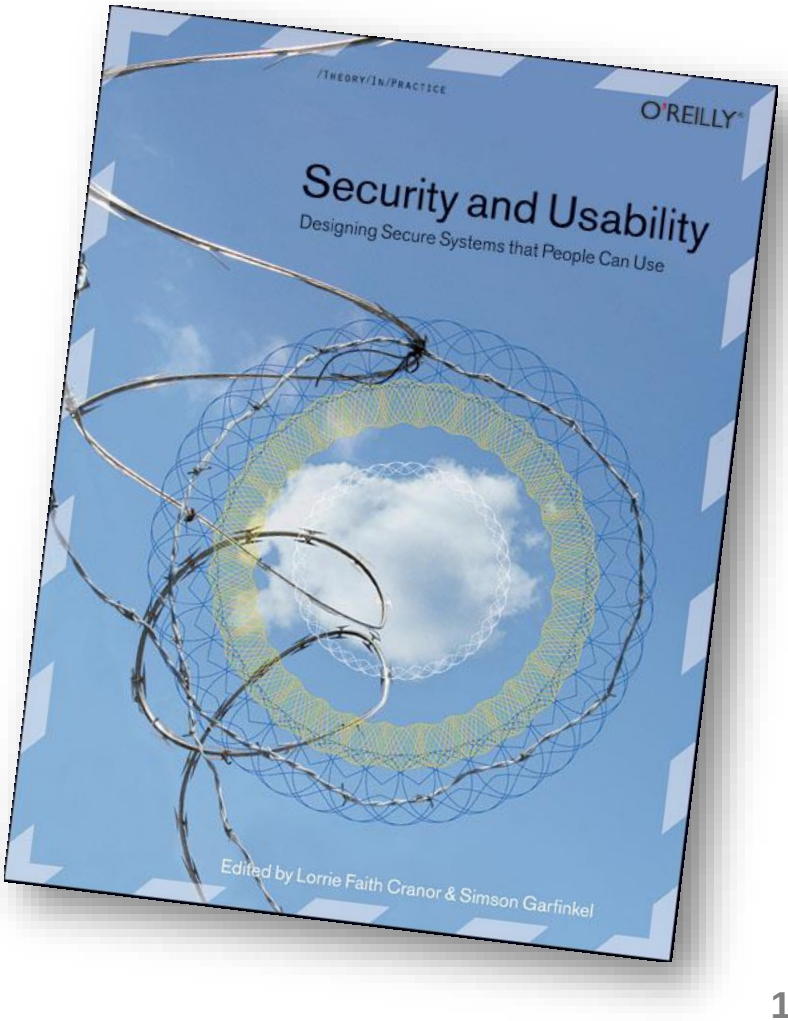
Unanticipated uses can bolster acceptance

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

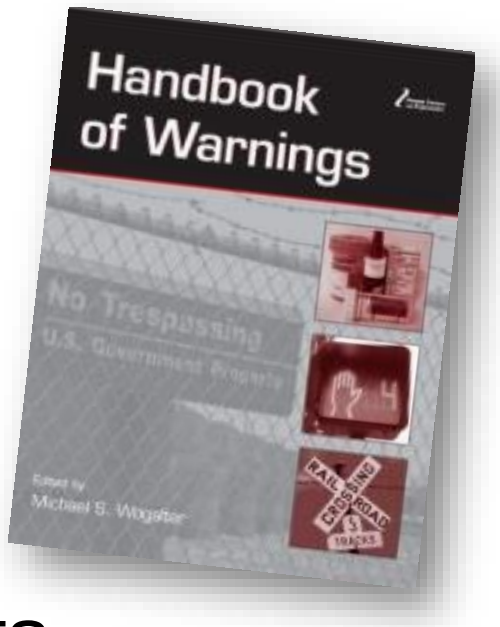


Try to better understand humans in the loop

- 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?

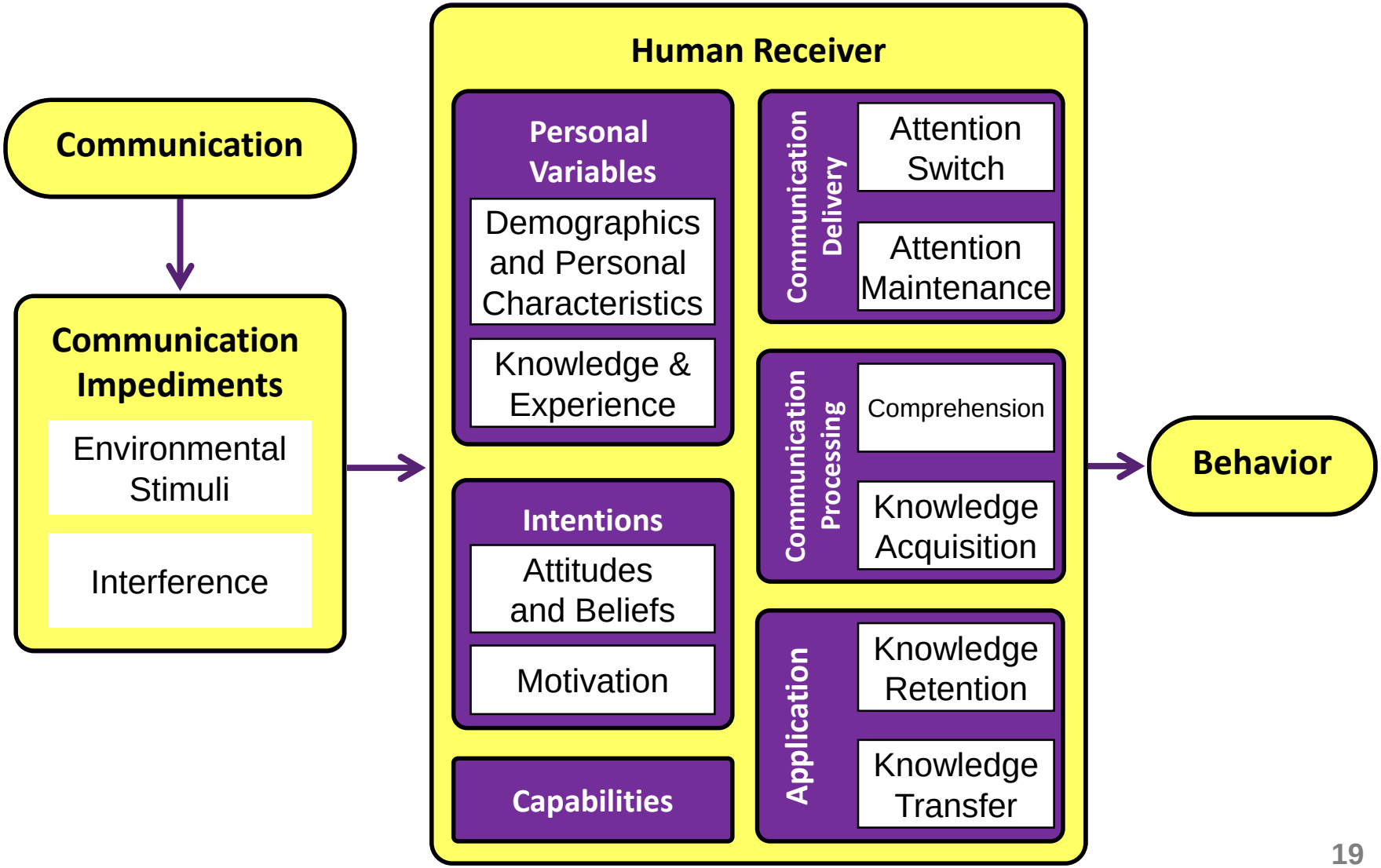
Human-in-the-loop framework

- Based on Communication-Human Information Processing Model (C-HIP) from Warnings Science
- Models human interaction with secure systems
- Can help identify human threats

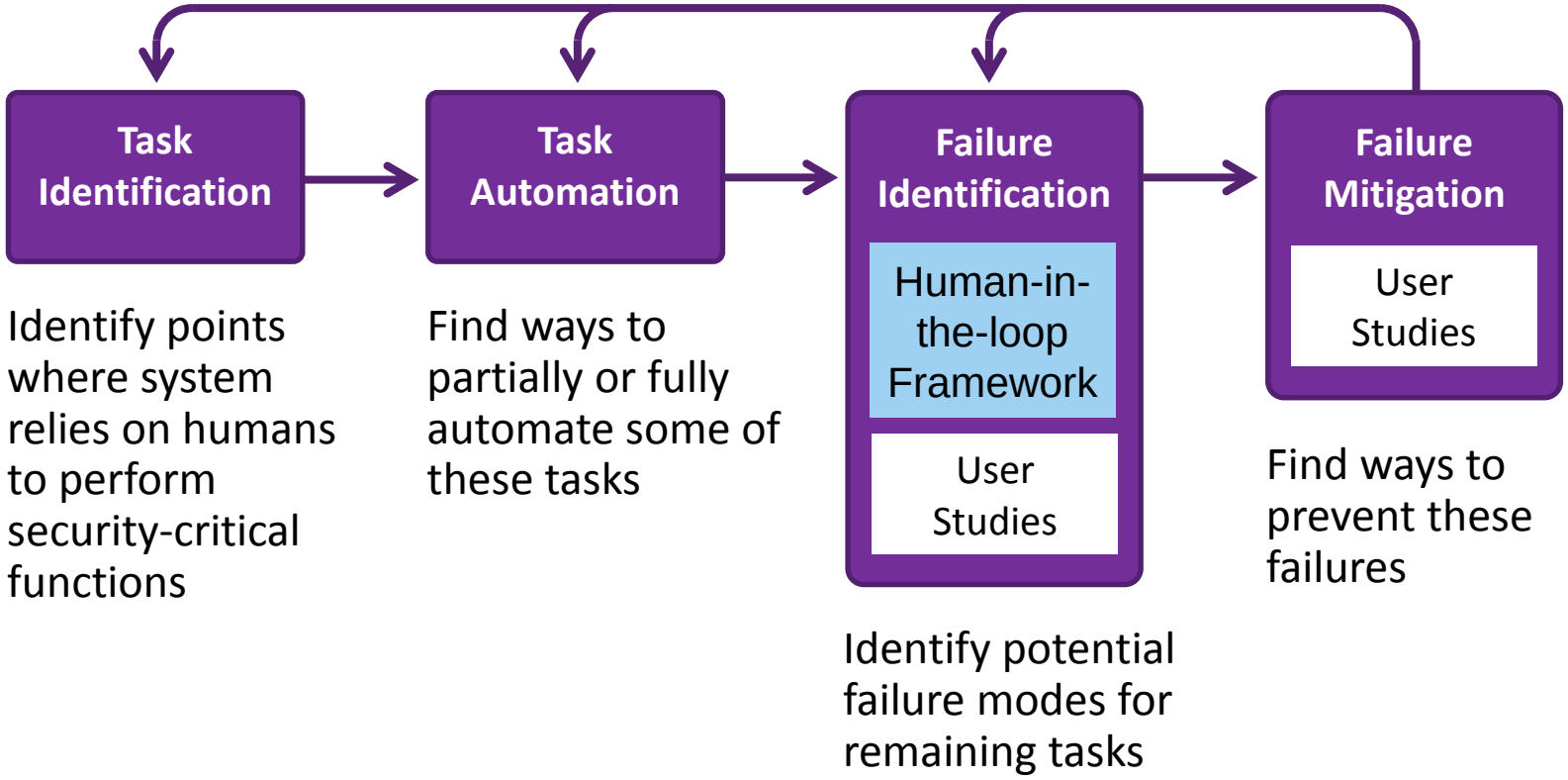


L. Cranor. A Framework for Reasoning About the Human In the Loop. Usability, Psychology and Security 2008.
http://www.usenix.org/events/upsec08/tech/full_papers/cranor/cranor.pdf

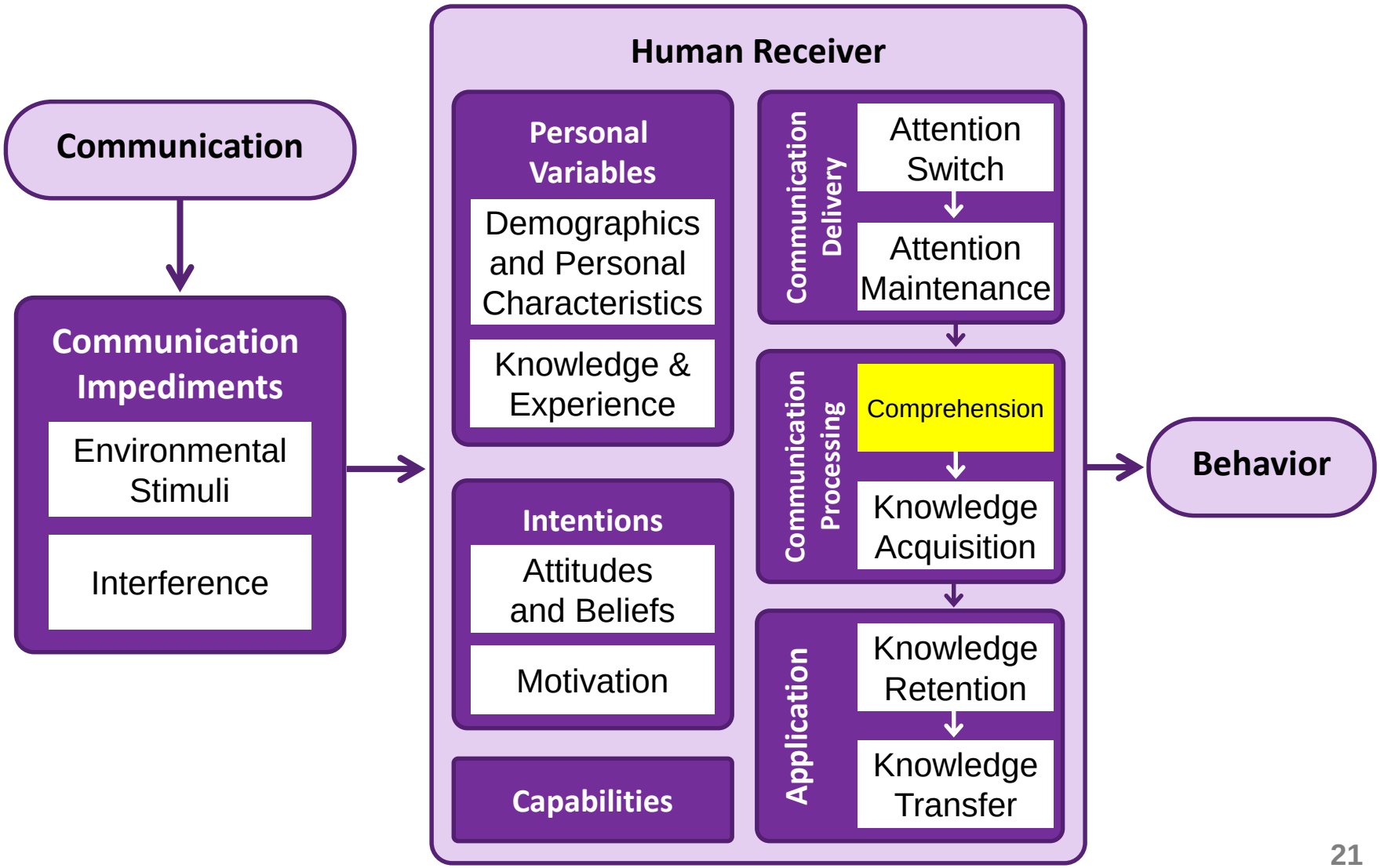
Human-in-the-loop framework

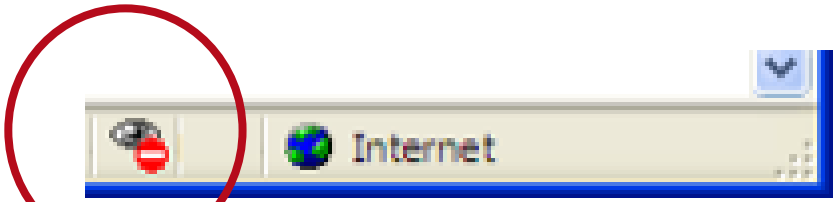


Human threat identification and mitigation process

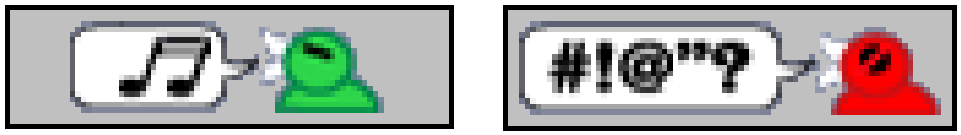


Human-in-the-loop framework





Internet Explorer cookie flag



Privacy policy ***matches*** user's privacy preferences

Privacy policy ***does not match*** user's privacy preferences

OPERATOR SPECIALTY COMPANY, INC.

ARNING

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


PRINCE HOTELS
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

Image courtesy of Johnathan Nightingale


What to do about hazards?


Best solution: remove hazard


Next best: guard against hazard

HOLE

STOP

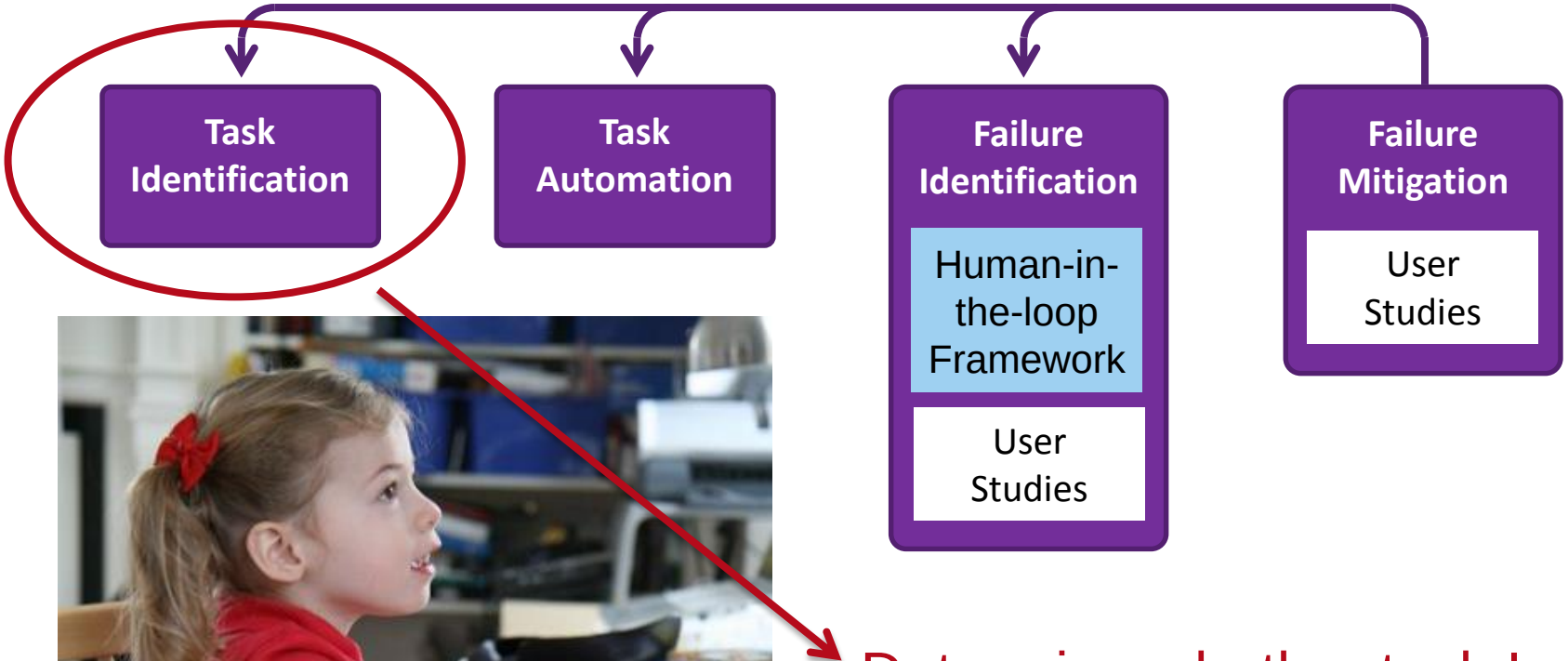
If all else fails: warn

CAUTION

CAUTION

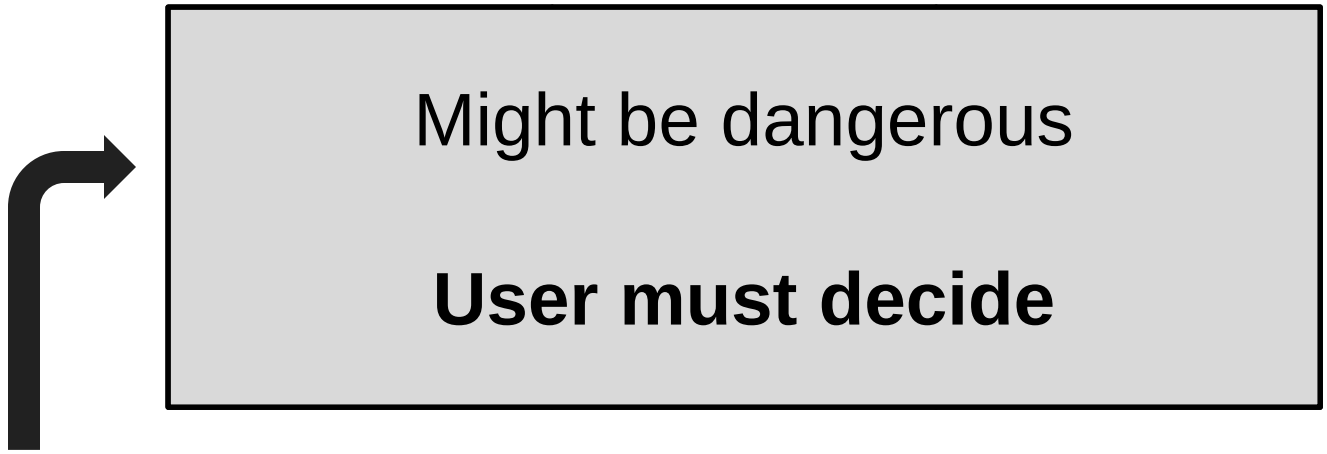

CAUTION UNEVEN SURFACES

Human threat mitigation for warnings



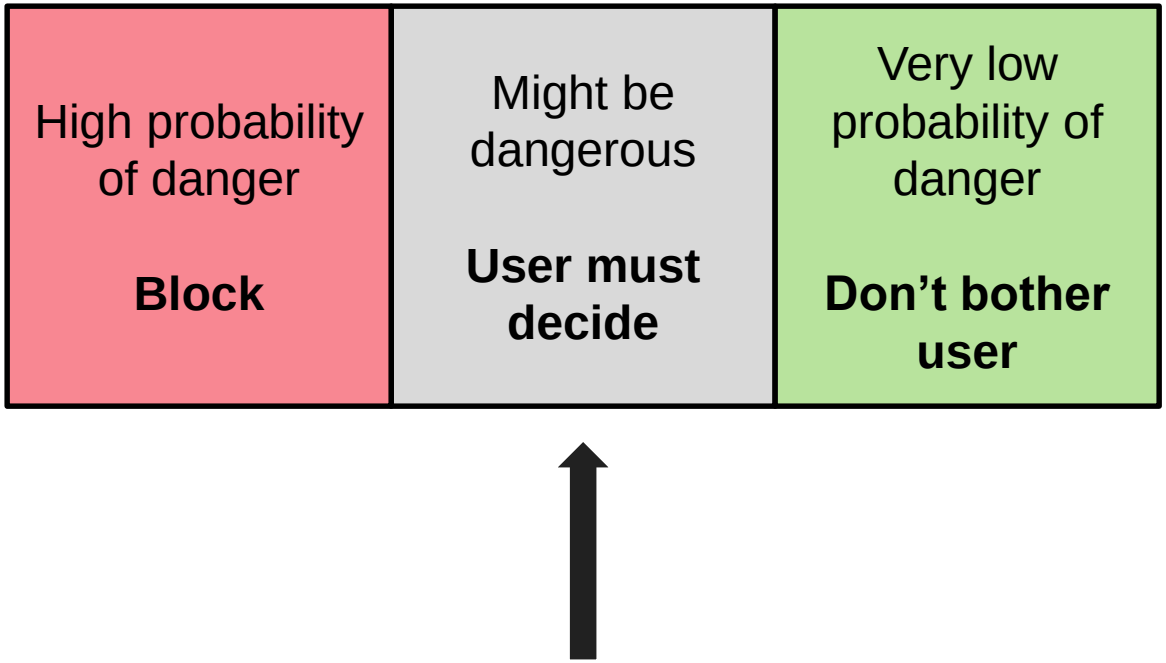
Determine whether task I am trying to complete is sufficiently risky that I should stop

Automate and change tasks to reduce need for user involvement



Use automated analysis to determine probability of danger

Support user decision



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


Life vest below center armrest
Fasten seat belt while seated

Unione Commercio Turismo
e Attività di Servizio

IN QUESTO LOCALE È

VIETATO FUMARE

RAUCHEN VERBOTEN

NO SMOKING


R3D085
bticino


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.


UNLOCKED ↓
LOCKED →


"THE PRIVACY COVER"
PATENT PENDING
www.theprivacycover.com


NO
YES

温水
便座
運転
着座センサー
水勢
乾燥
ビデ
おしり
止
ムーブ入/切
ムーブ入/切


STOP
REAR CLEANSING
FRONT CLEANSING
PRESSURE
TEMPERATURE
HIGH
LOW
SEAT
ENERGY SAVER
TIMER
AUTO
WAND CLEANING
POWER

ON
LOW POWER
WAIT
杀菌
消毒
Please press the ON button.
更换一次性便洁套，请按ON键

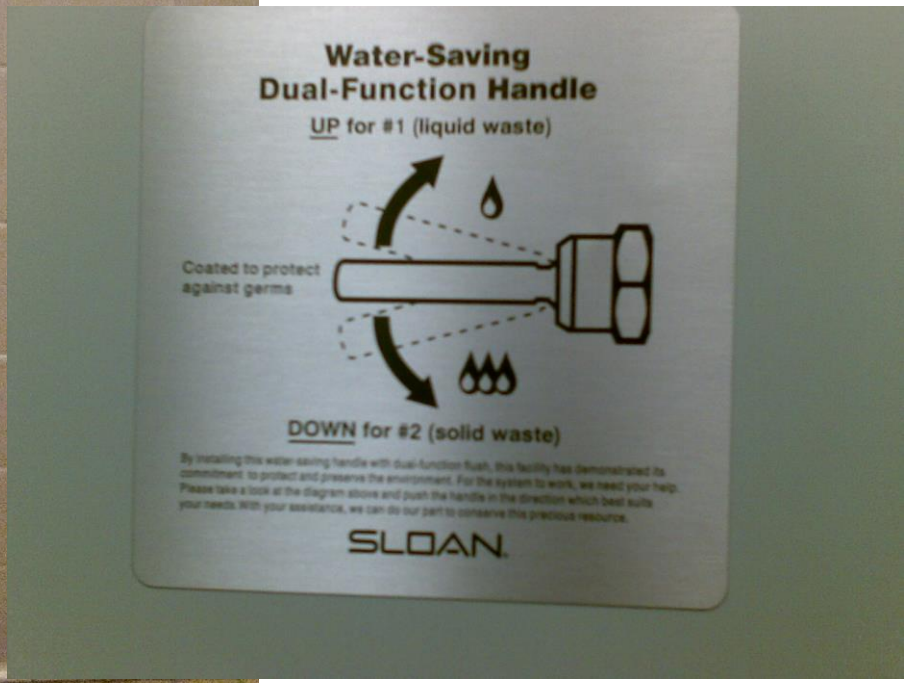

PLEASE NOTE THAT
THIS FACILITY IS NOT
EQUIPPED WITH AN
AUTOMATIC FLUSHING
SYSTEM.
PLEASE FLUSH PRIOR
TO LEAVING THE
STALL.
THANK YOU FOR YOUR COOPERATION.
CBRE
CB RICHARD ELLIS


NOTICE
Should Commode Not
Clear Completely,
Operate Flush valve
By Pushing the Black Button


COURTESY MANUAL FLUSH BUTTON
E-Z FLUSH
PRESS
COURTESY MANUAL
FLUSH BUTTON
IF NOT WORKING CORRECTLY PLEASE
ADDRESS TO FACILITIES IMMEDIATELY
CALL X54000


If toilet does not flush automatically before
you exit the stall, please press button on the
side of the cylinder to flush.


Water-Saving
Dual-Function Handle
UP for #1 (liquid waste)
Coated to protect
against germs
DOWN for #2 (solid waste)
SLOAN


Water-Saving
Dual-Function Handle
UP for #1 (liquid waste)
Coated to protect
against germs
DOWN for #2 (solid waste)
SLOAN


Clean dispenser with a soft wiper and mild soap & water.
pie la distribuidora con un paño fino, agua y un detergente s
Nettoyer la boîte distributrice á l'aide d'un chiffon doux et
l'eau savonneuse


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.


NOTICE
NON-POTABLE WATER
NOT FOR DRINKING
OR COOKING USE
AVISO
AGUA NO POTABLE
NO APTA PARA BEBER
NI COCINAR
Please Deposit
All
Sanitary Napkins


This bathtub has been treated with snash
2000 anti-slip substance for your safety
אמבטיה זו עברה טיפול סנאש 2000
למניעת החלקה לביטחונך האישי
SNASH
SNASH int Markating סנאש שיווק בינלאומי בע"מ
Tel.972-3-5748483 טל.


FOR SHOWER:
TURN ON WATER
ADJUST TEMPERATURE
PULL DOWN SPOUT RING
SPOUT RING

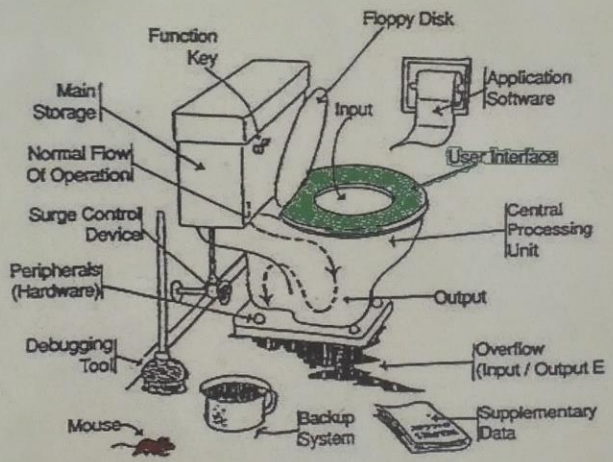
IF THIS RESTROOM IS
IN NEED OF ATTENTION,

PLEASE CALL:
225-4141

PLEASE USE THE FOLLOWING
IDENTIFIER FOR THIS RESTROOM:
C2B1

HOUSE SUPERINTENDENT'S OFFICE

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 age20-29 age30-39 age40-49 age50-59 age60-69 age90-99 alone alone/private space anonymous away from family bank statement basement bathing bathroom bedroom big brother blanket bow box brain browser