03- Reasoning about the Human in the Loop

Lorrie Cranor and Blase Ur

January 21, 2014

05-436 / 05-836 / 08-534 / 08-734
Usable Privacy and Security

Carnegie Mellon University
CyLab

isr institute for SOFTWARE RESEARCH

Engineering & Public Policy

Today!

- Finish HCI methods (10 min.)
- Discussion of the Johnnys (15 min.)
- Human in the Loop Framework (35 min.)
- The other side of the story (10 min.)
- “Users are not the enemy” (10 min.)

Create your plan

- Develop hypotheses
- Develop protocol
  - Exact steps
  - Exactly what you will say
  - Will you record audio / screen capture?
  - What will you write down? Make a template
  - Have a plan for analysis
- Develop system

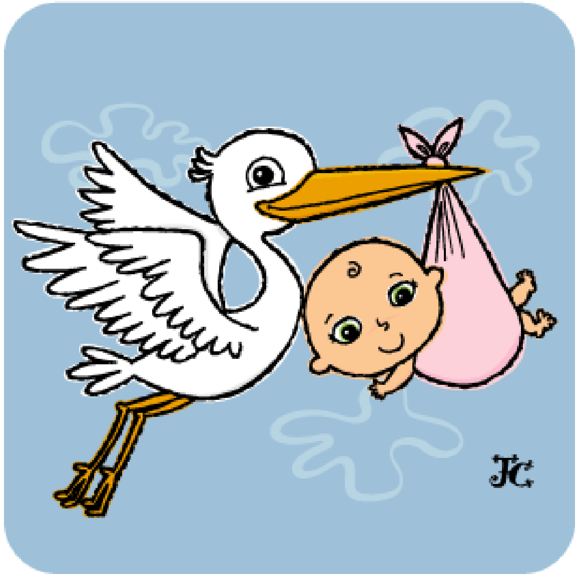
Pilot test and iterate

- Run through the whole study with members of the research team
- Run through the whole study with friends
- Do some preliminary data analysis
- Revise things that are confusing, take too long, or are unrelated to your goals
- Repeat

Always be ethical

- Studies can be distressing
  - Users have left in tears
  - No one likes to feel tricked
  - Make sure participants understand *why*
- The onus is on the researcher
  - **Informed consent**, voluntary procedures
  - They can stop at any time (fully paid)
  - You are testing the system, not them
  - Make collected data anonymous

Where do study participants come from?



Recruiting participants

- Posters, Craigslist, participant pools, specialized email lists/forums, MTurk
- How much of the study do you reveal?
- Tell them (and remind them) where they're going and parking, and how to contact you
- Reserve appropriate space
  - Be there early, have supplies and payment

Analyze data

- Keep it safe (encrypted, locked)
- Make backup copies
- Summarize key points after interviews
- Code qualitative data
- Visualize data and run statistical tests
- Iterate
  - Do another study? Do another analysis?

Report your methodology (1/2)

- Assumptions, threat model
- How were participants recruited?
- What incentive / compensation was there?
- Where did the study take place?
- What instructions were given?
- What was the procedure?
- What were the treatments/conditions?

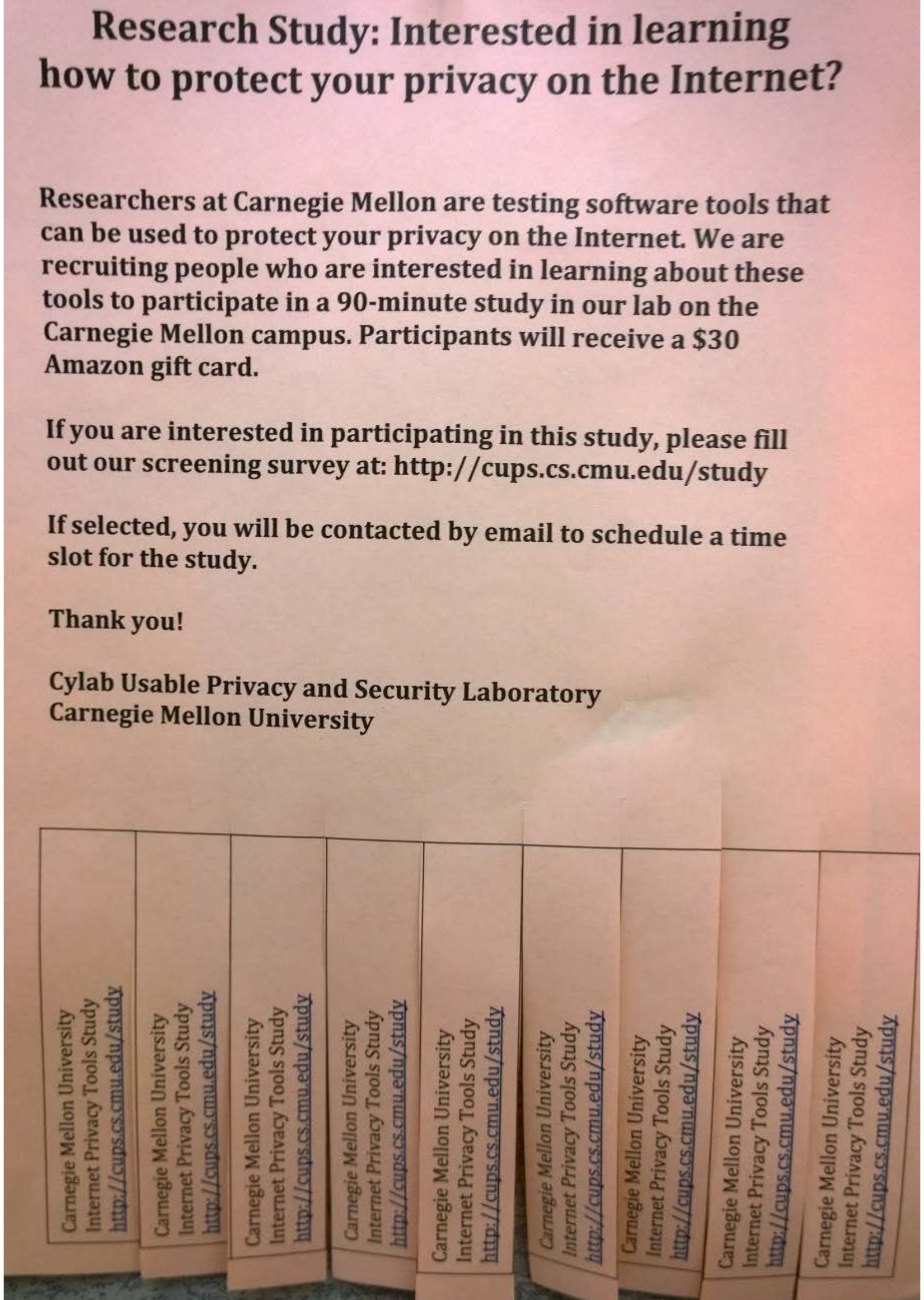
Report your methodology (2/2)

- What did participants learn along the way?
- Did the order of tasks vary?
- Describe your analysis methods
  - How did you choose them?
  - Correlation is not causation!
  - How did you code qualitative data?
- What are your limitations and biases?
- Have others used this methodology?

Why Johnny can’t do anything right

Example: *Why Johnny Can't Opt Out*

- Backstory
- Study design
- Study materials
- Results



Research Study: Interested in learning how to protect your privacy on the Internet?

Researchers at Carnegie Mellon are testing software tools that can be used to protect your privacy on the Internet. We are recruiting people who are interested in learning about these tools to participate in a 90-minute study in our lab on the Carnegie Mellon campus. Participants will receive a $30 Amazon gift card.

If you are interested in participating in this study, please fill out our screening survey at: http://cups.cs.cmu.edu/study

If selected, you will be contacted by email to schedule a time slot for the study.

Thank you!

Cylab Usable Privacy and Security Laboratory
Carnegie Mellon University

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Carnegie Mellon University
Internet Privacy Tools Study
http://cups.cs.cmu.edu/study

Tips from this study

- Be prepared for early/thirsty participants
- Make backup recording
- Setting browser/machine to clean state
- Have a good way to take notes
- Script any scenarios you can think of

In groups of 2 or 3 people discuss:

- What are the general usability lessons from each of the Johnny papers?
  - Example: “Make the status of the system obvious to users”

Why can’t Johnny opt out?

- Jargon
- Bad defaults
- Incorrect mental model of OBA/tool
- Many steps
- Slow
- Status of system not obvious
- Didn’t know where to go next

Why can’t Johnny encrypt?

- Bad visual metaphors (pen, old/new keys)
- People-based, not key-based
- Key server opaque to users
- The meaning of “validity” and “trust”
- Irreversible actions (consequences)
- Inconsistency: “currently encoding”
- Too much information

Why didn’t Johnny encrypt?

- Emailed secret unencrypted
- Unable to encrypt/decrypt at all
- Public key model misunderstood
  - P5 generated key pairs for others
- Getting others’ keys was difficult
- Unaware that they had not revoked key
- Unsure about trust

The Human in the Loop

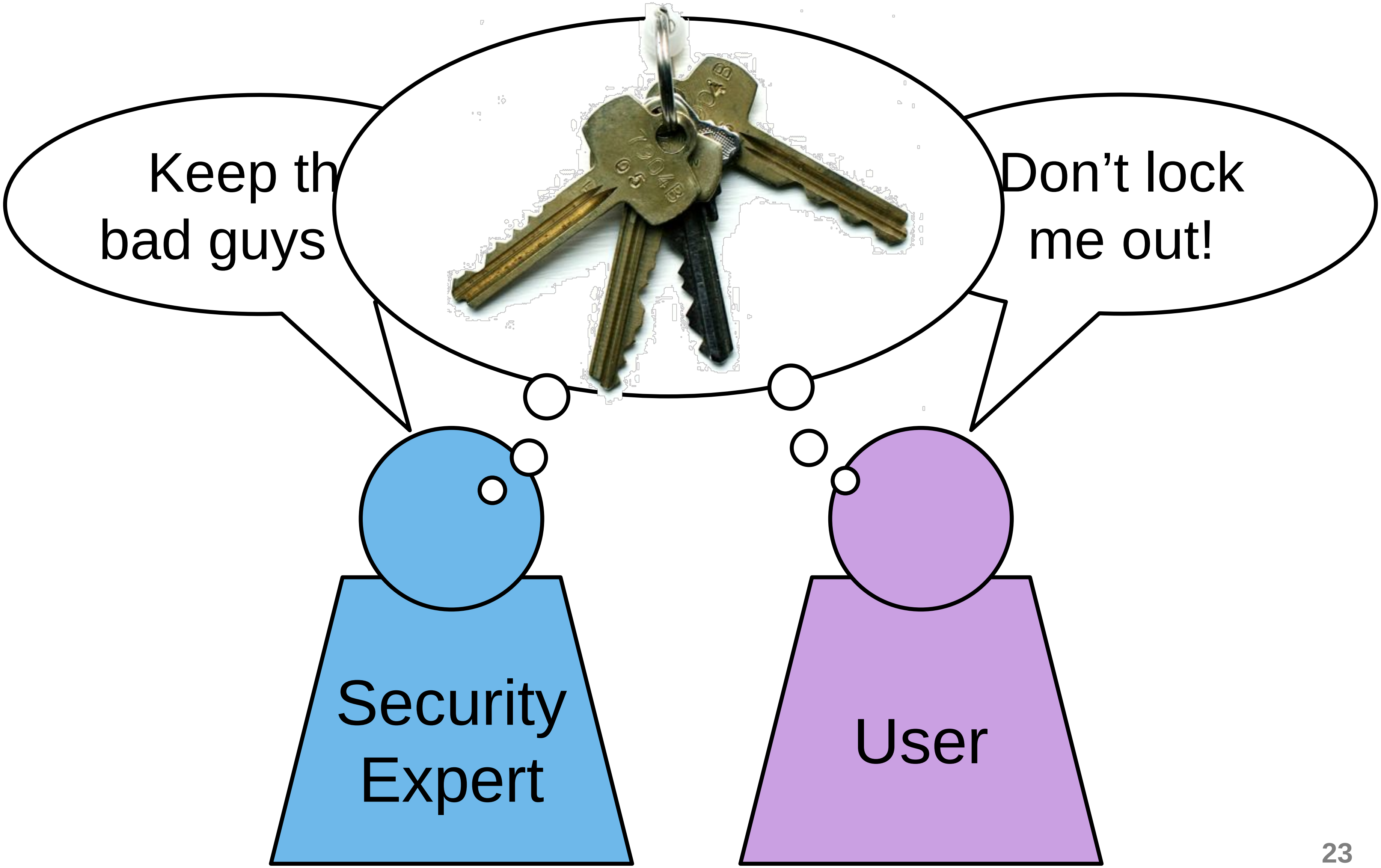
The human threat

- 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 th
bad guys

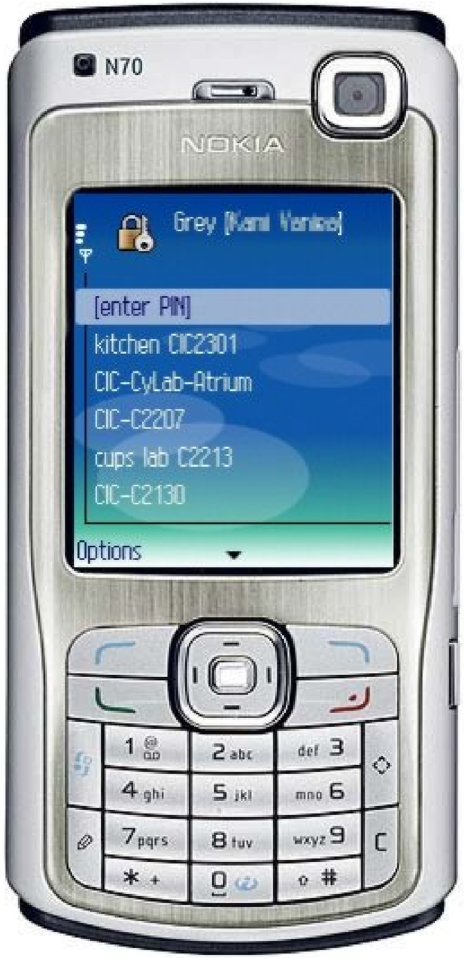
Don’t lock
me out!

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

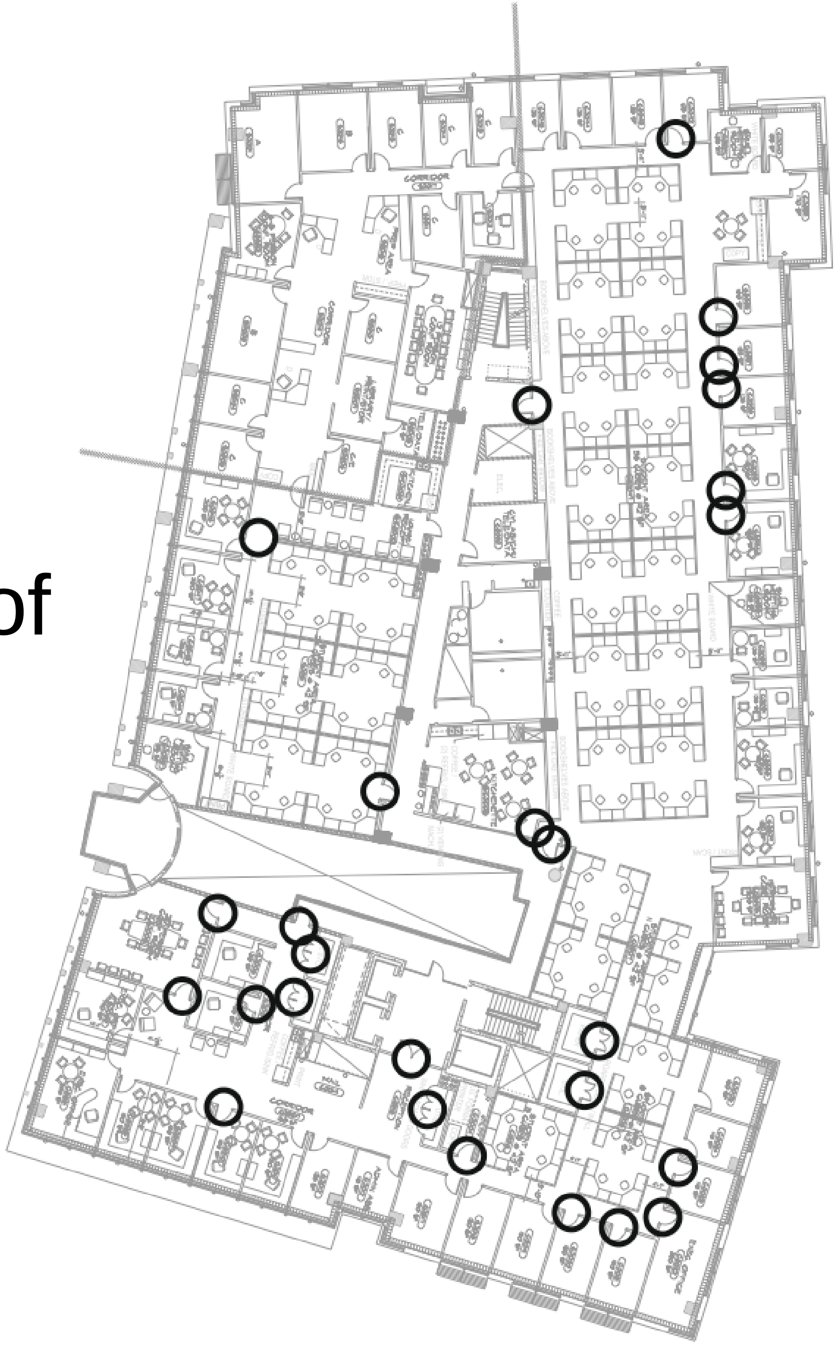


L. Bauer, L.F. Cranor, R.W. Reeder, M.K. Reiter, and K. Vaniea. **A User Study of Policy Creation in a Flexible Access-Control System.** CHI 2008. http://www.robreeder.com/pubs/greyCHI2008.pdf

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

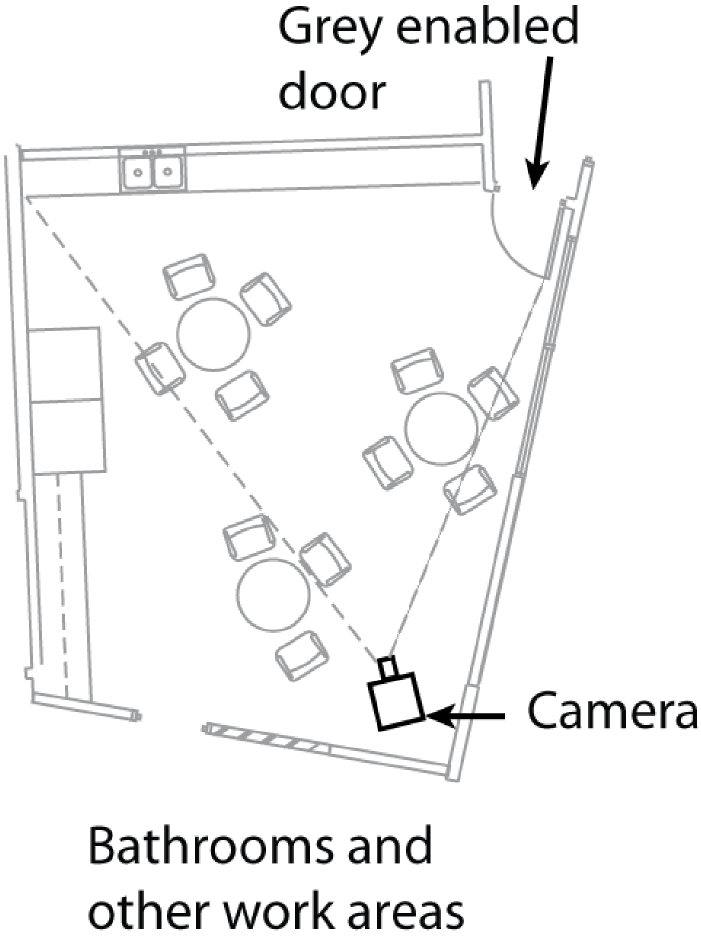
Data collection

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

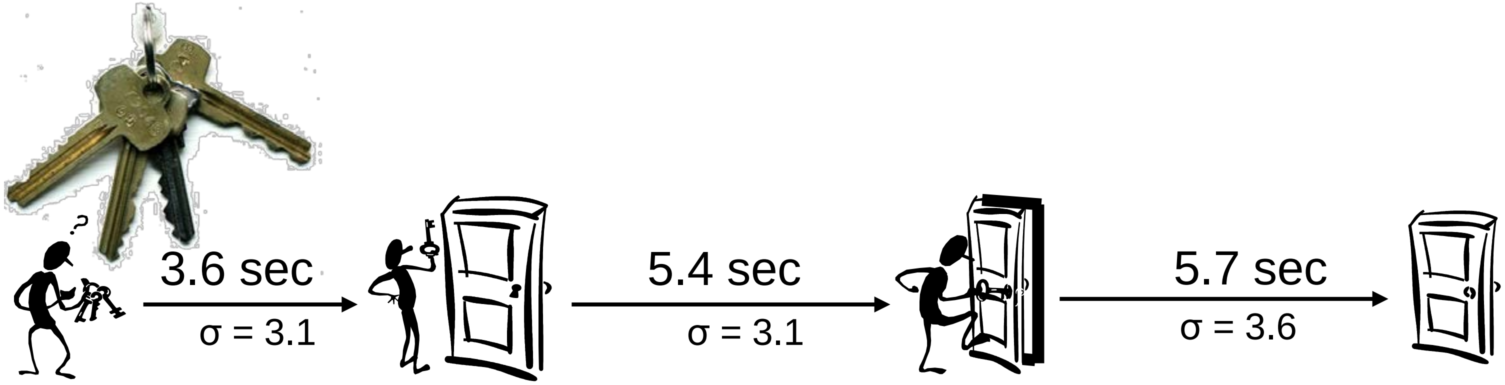


Users complained about speed

- 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



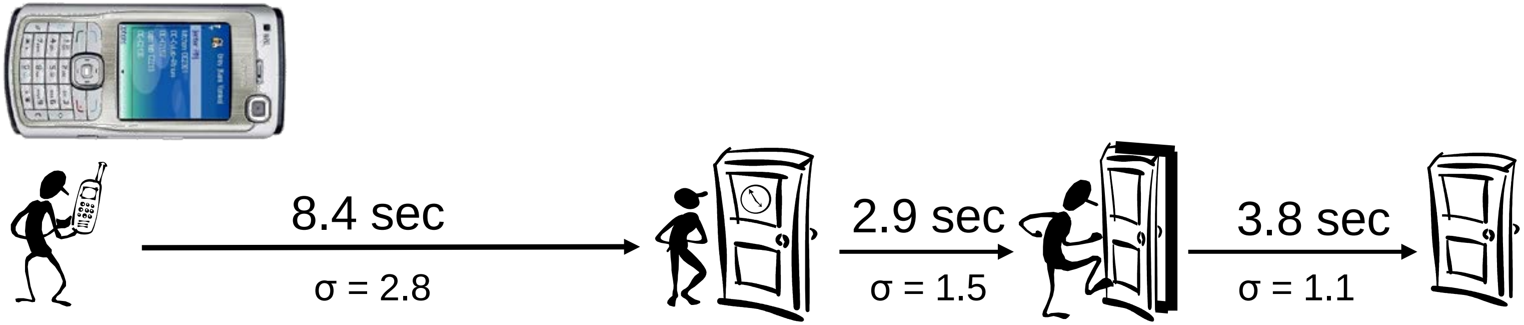
Average access times



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



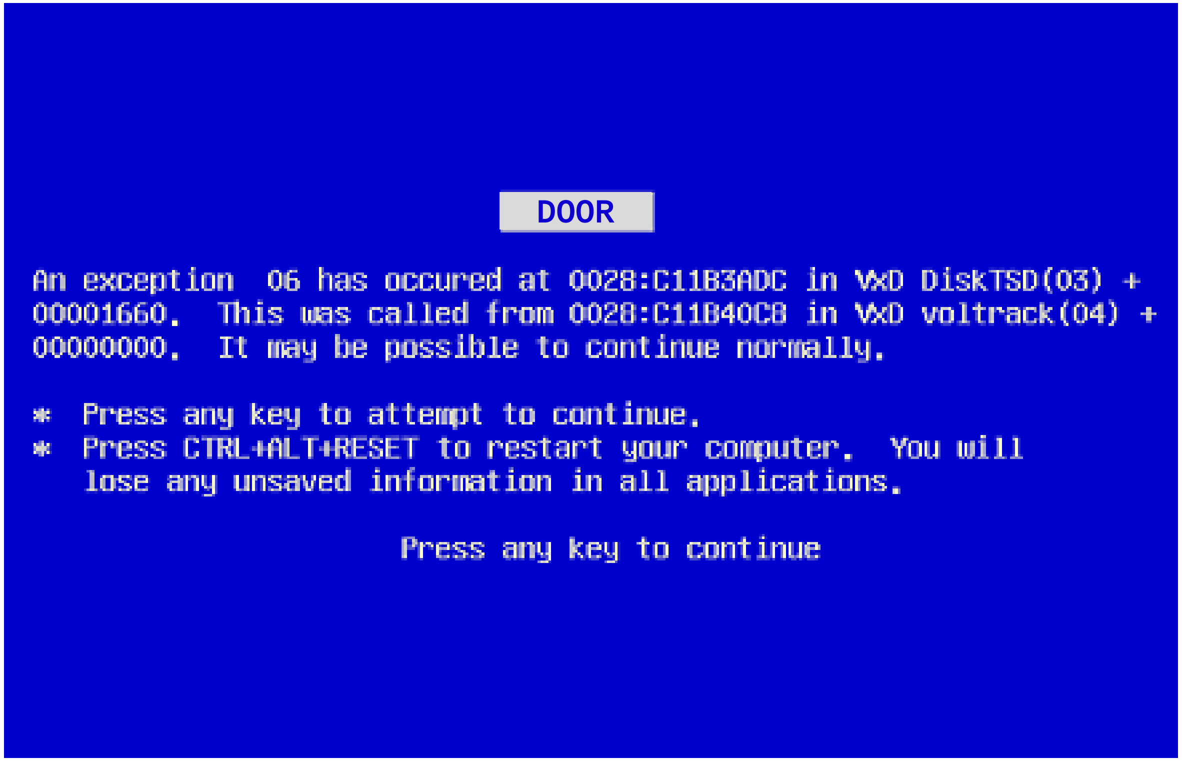
Getting phone → 8.4 sec, σ = 2.8 → Stop in front of door → 2.9 sec, σ = 1.5 → Door opened → 3.8 sec, σ = 1.1 → Door Closed

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.”

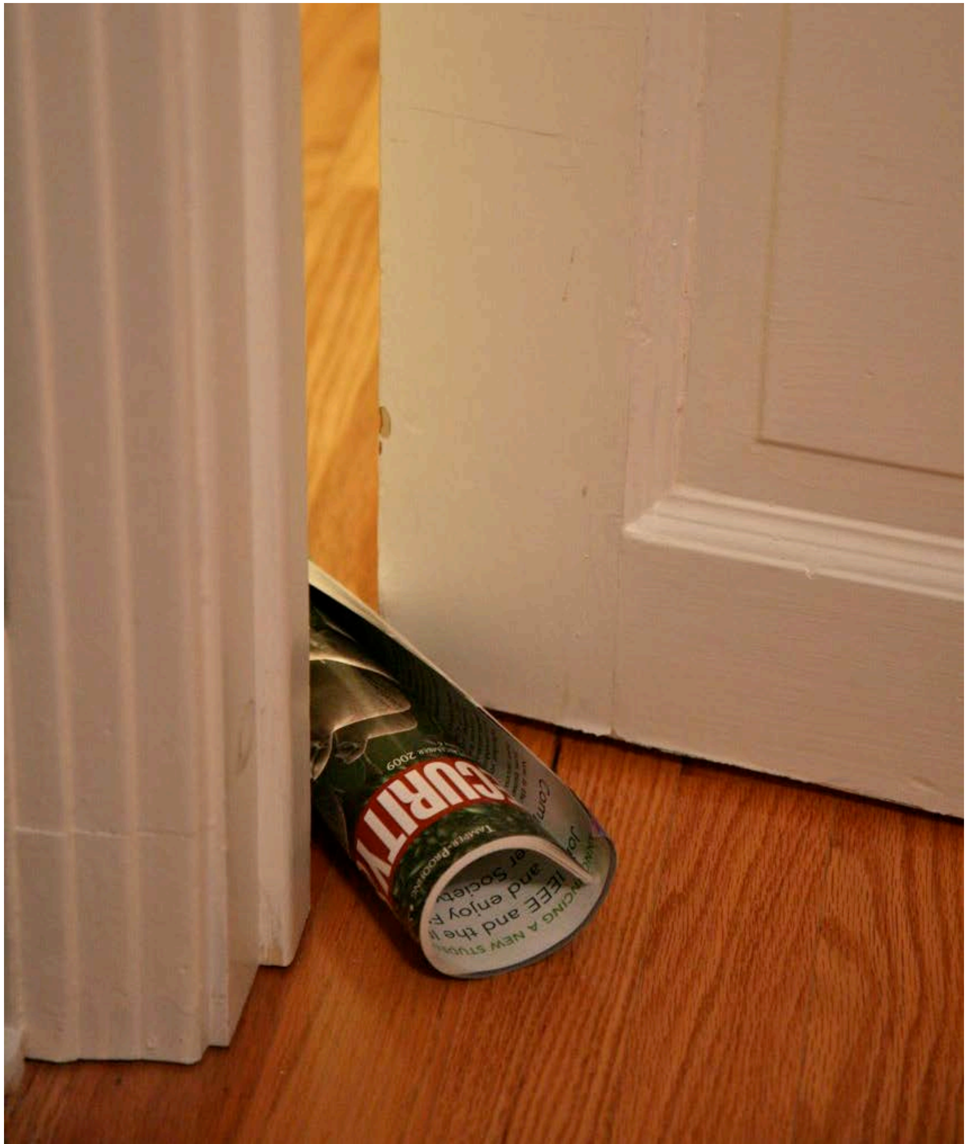
Nobody wants to have to reboot their door



```
                              DOOR

An exception  06 has occured at 0028:C11B3ADC in VxD DiskTSD(03) +
00001660.  This was called from 0028:C11B40C8 in VxD voltrack(04) +
00000000.  It may be possible to continue normally.

*  Press any key to attempt to continue.
*  Press CTRL+ALT+RESET to restart your computer.  You will
   lose any unsaved information in all applications.

                      Press any key to continue
```

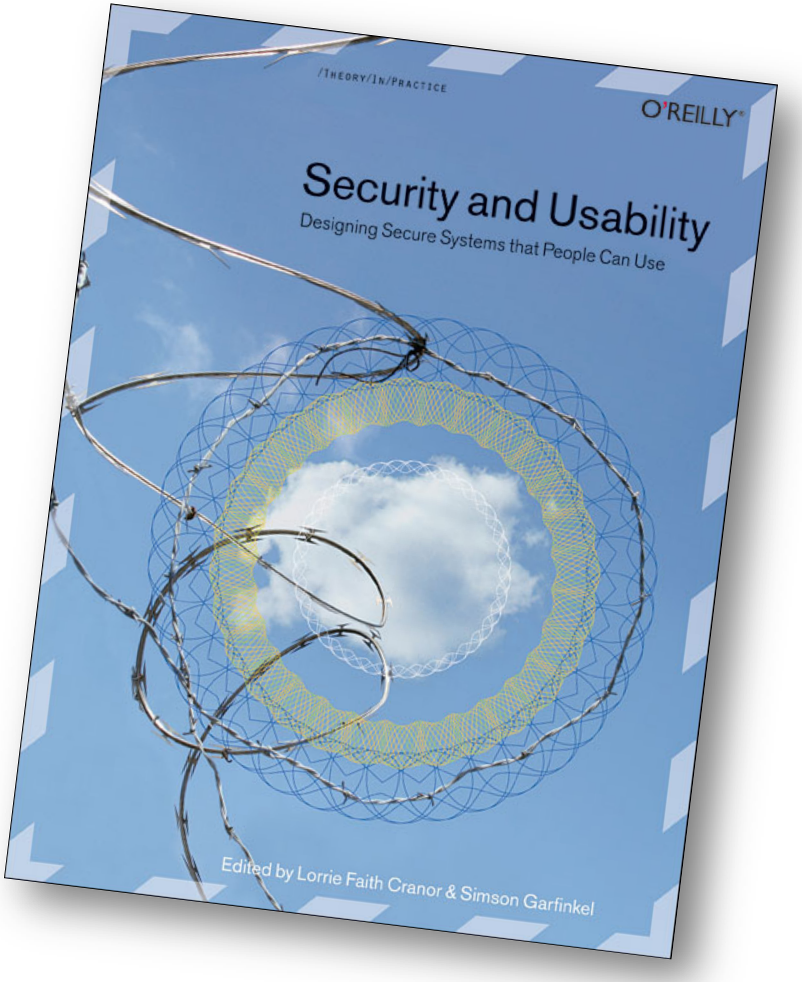
Unanticipated uses can bolster acceptance

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


/THEORY/IN/PRACTICE
O'REILLY
Security and Usability
Designing Secure Systems that People Can Use
Edited by Lorrie Faith Cranor & Simson Garfinkel

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?

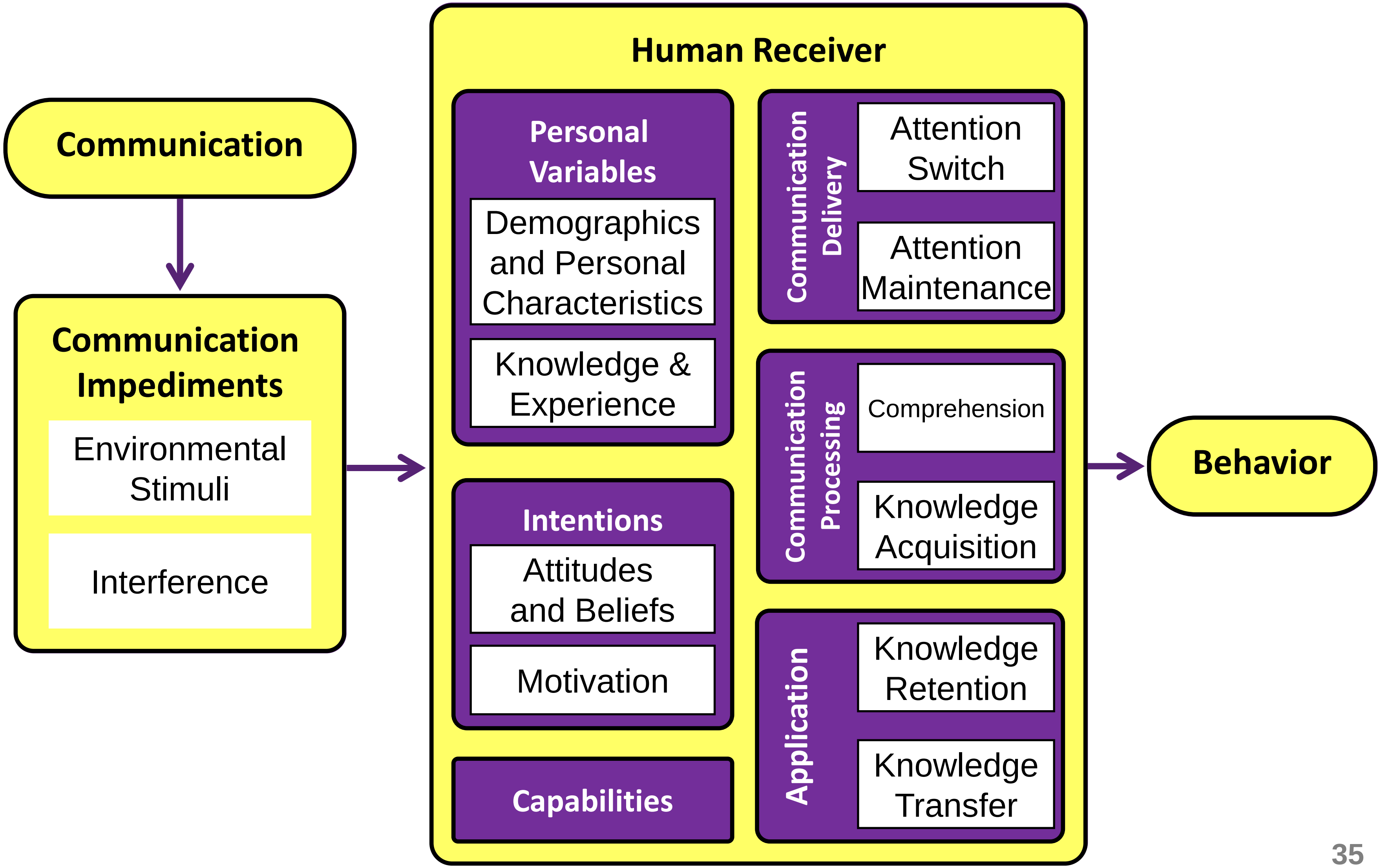
Human-in-the-loop framework

- 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


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

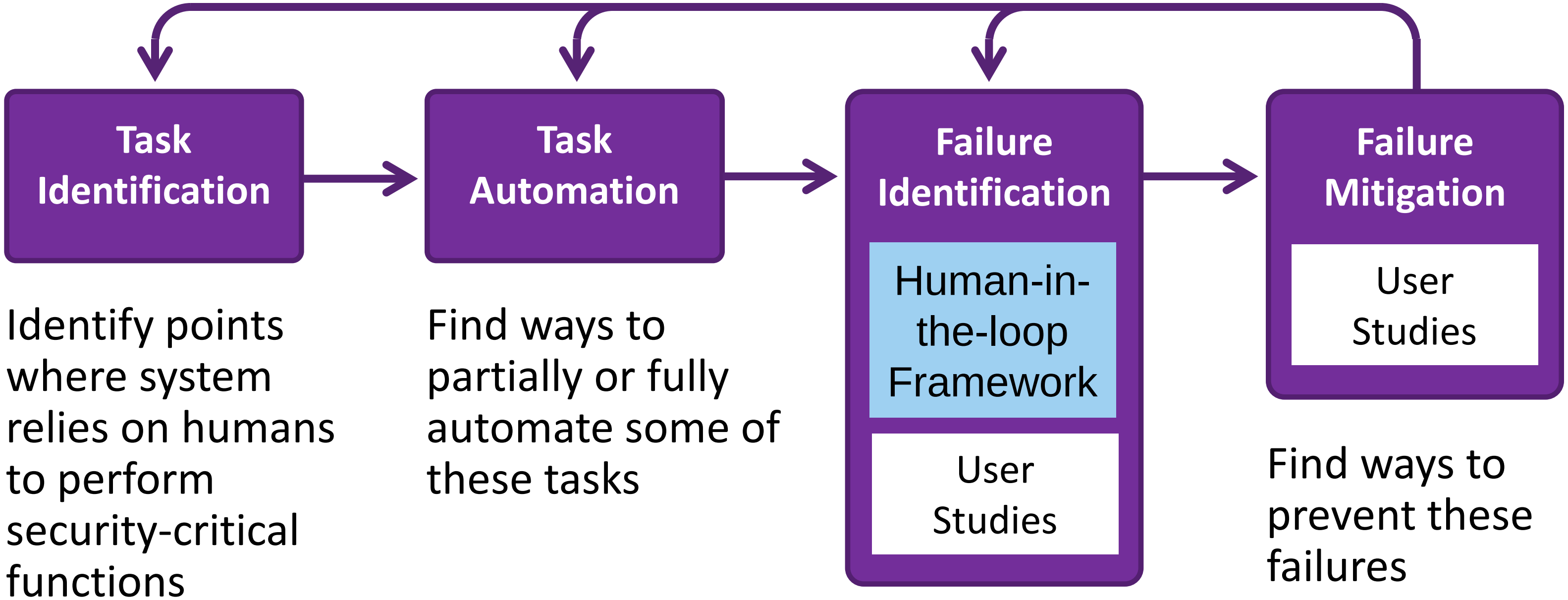
Application

Knowledge Retention

Knowledge Transfer

Behavior

Human threat identification and mitigation process



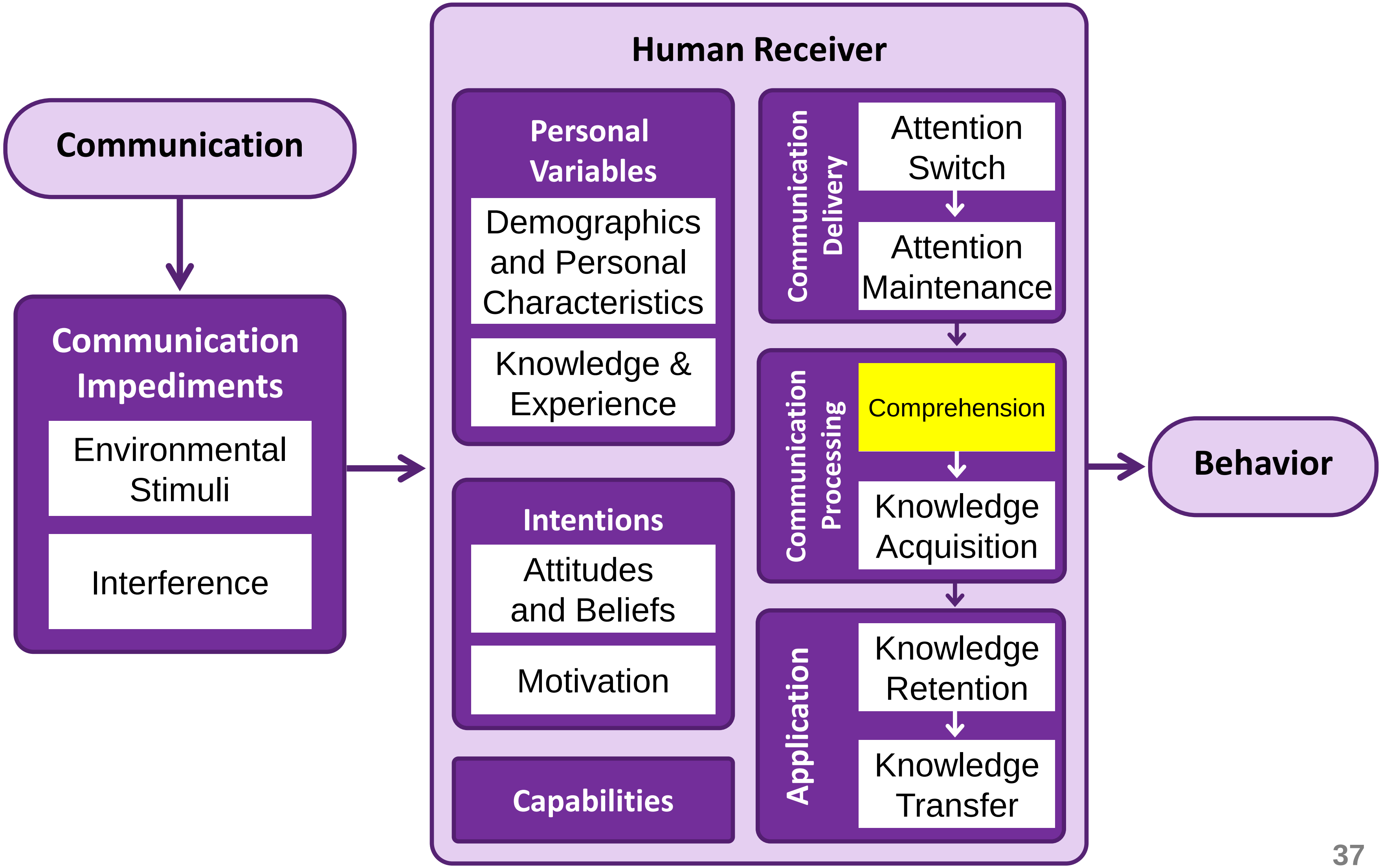
Identify points where system relies on humans to perform security-critical functions

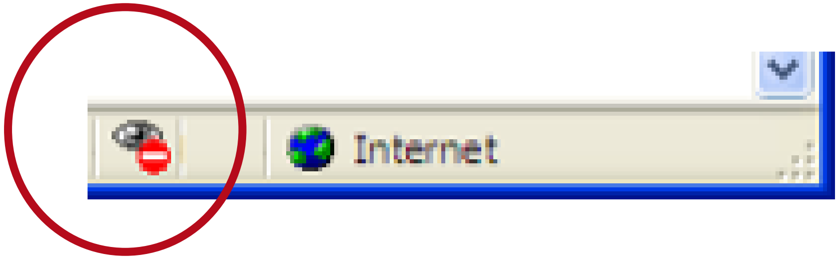
Find ways to partially or fully automate some of these tasks

Identify potential failure modes for remaining tasks

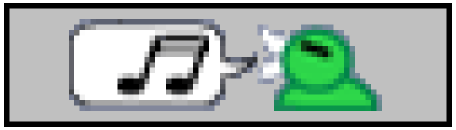
Find ways to prevent these failures

Human-in-the-loop framework

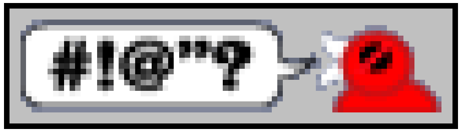




Internet Explorer cookie flag

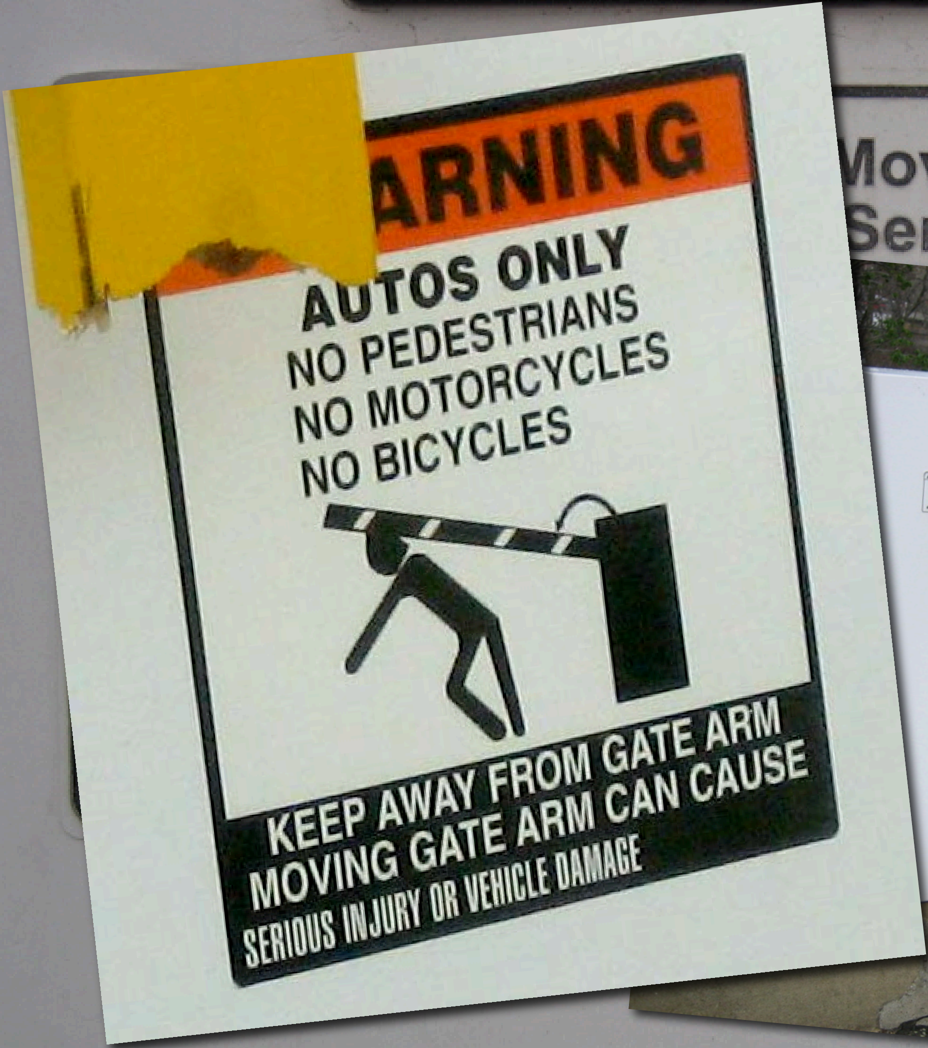


Privacy policy ***matches*** user’s privacy preferences



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

OPERATOR SPECIALTY COMPANY, INC.

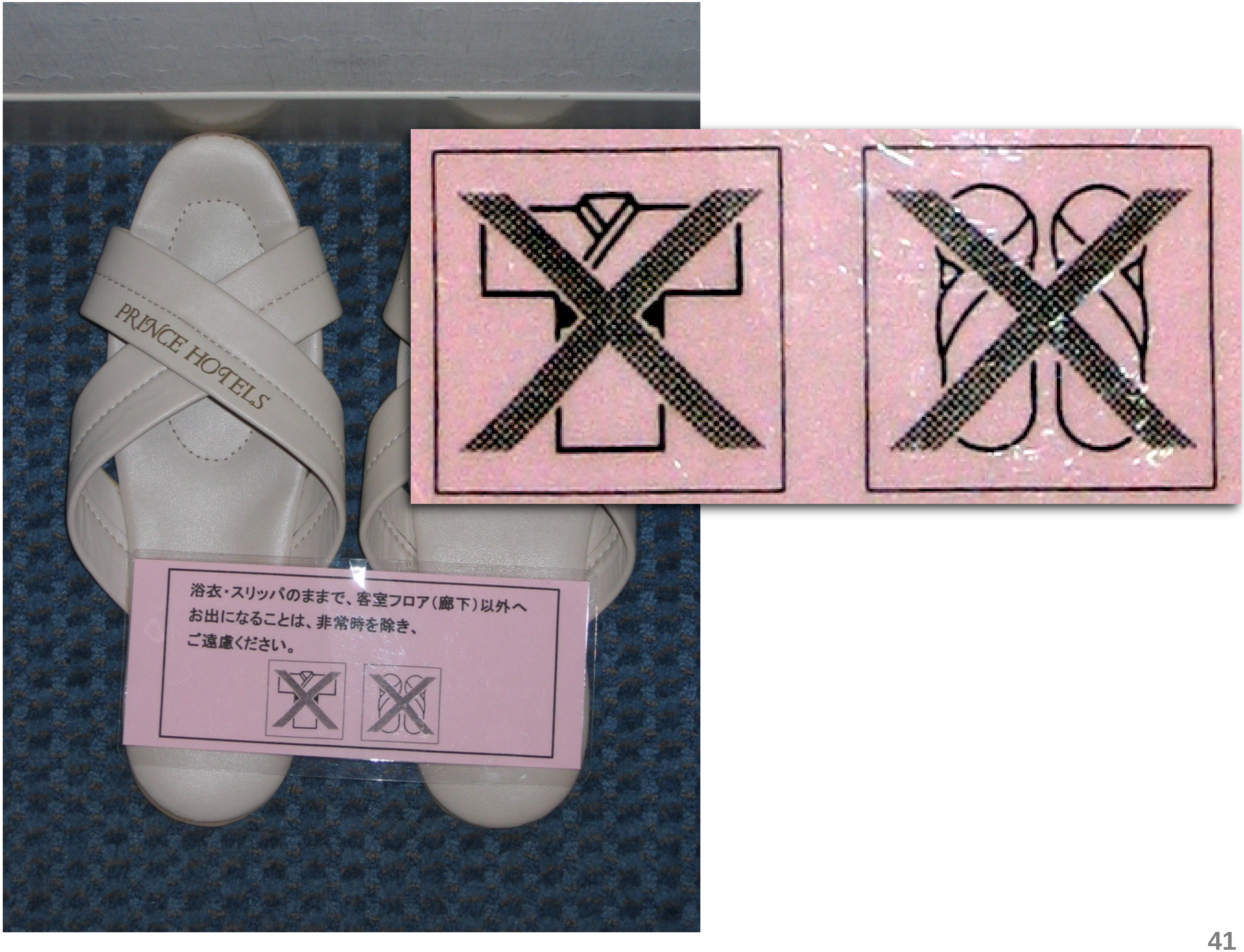


ARNING

AUTOS ONLY
NO PEDESTRIANS
NO MOTORCYCLES
NO BICYCLES

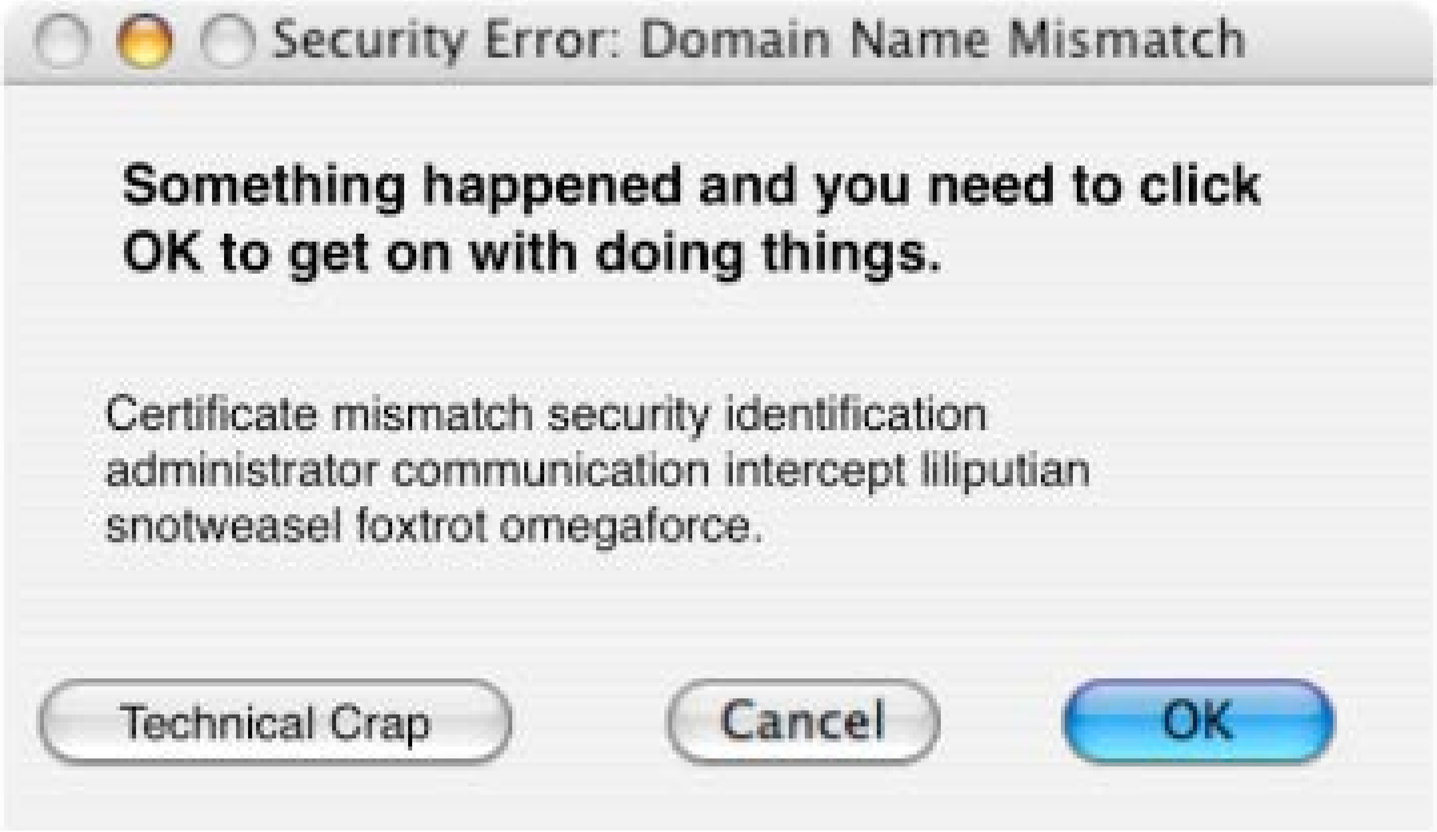
KEEP AWAY FROM GATE ARM
MOVING GATE ARM CAN CAUSE
SERIOUS INJURY OR VEHICLE DAMAGE

Moving Gate Can Cause
Serious Injury or Death



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

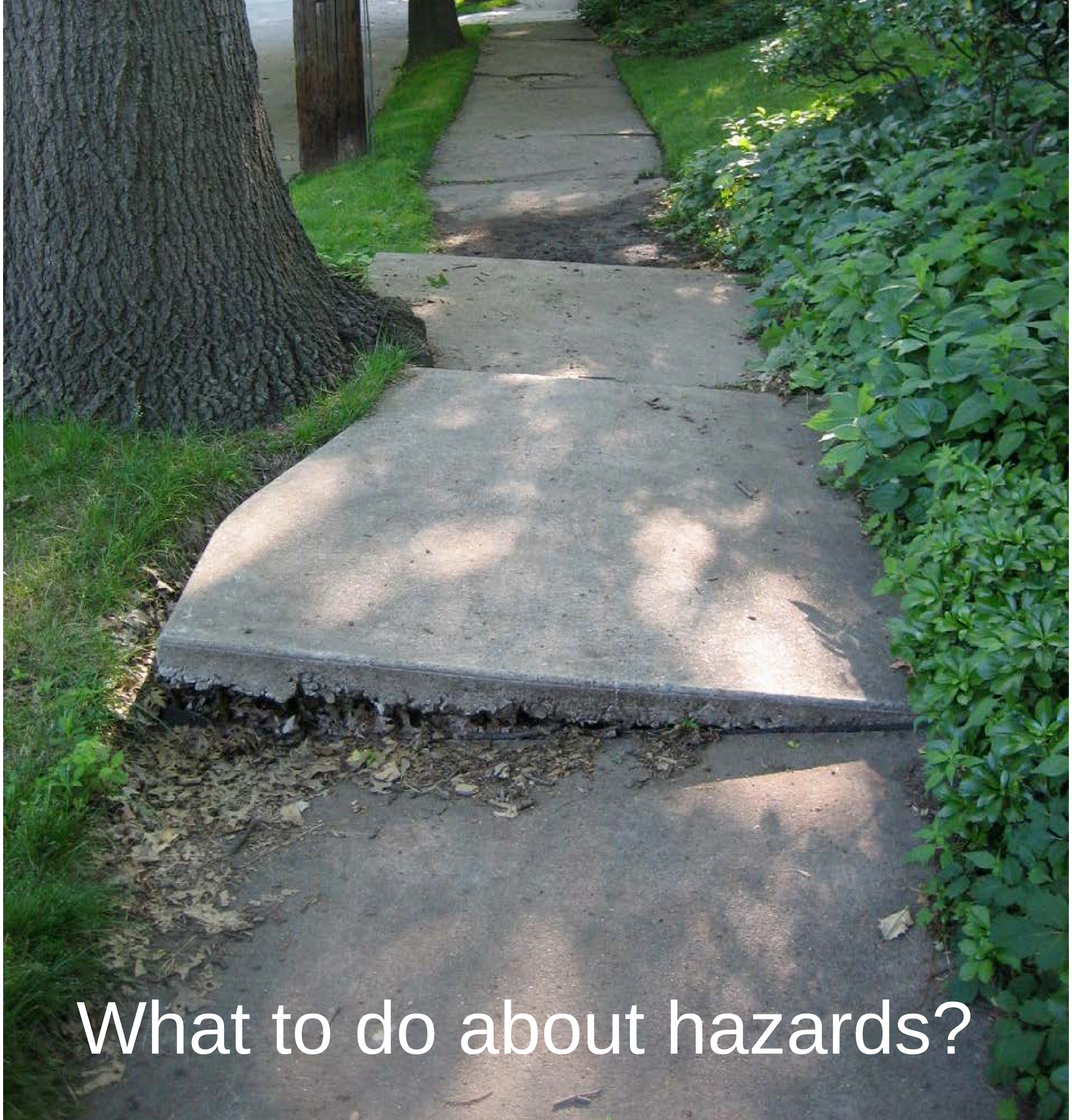


Security Error: Domain Name Mismatch

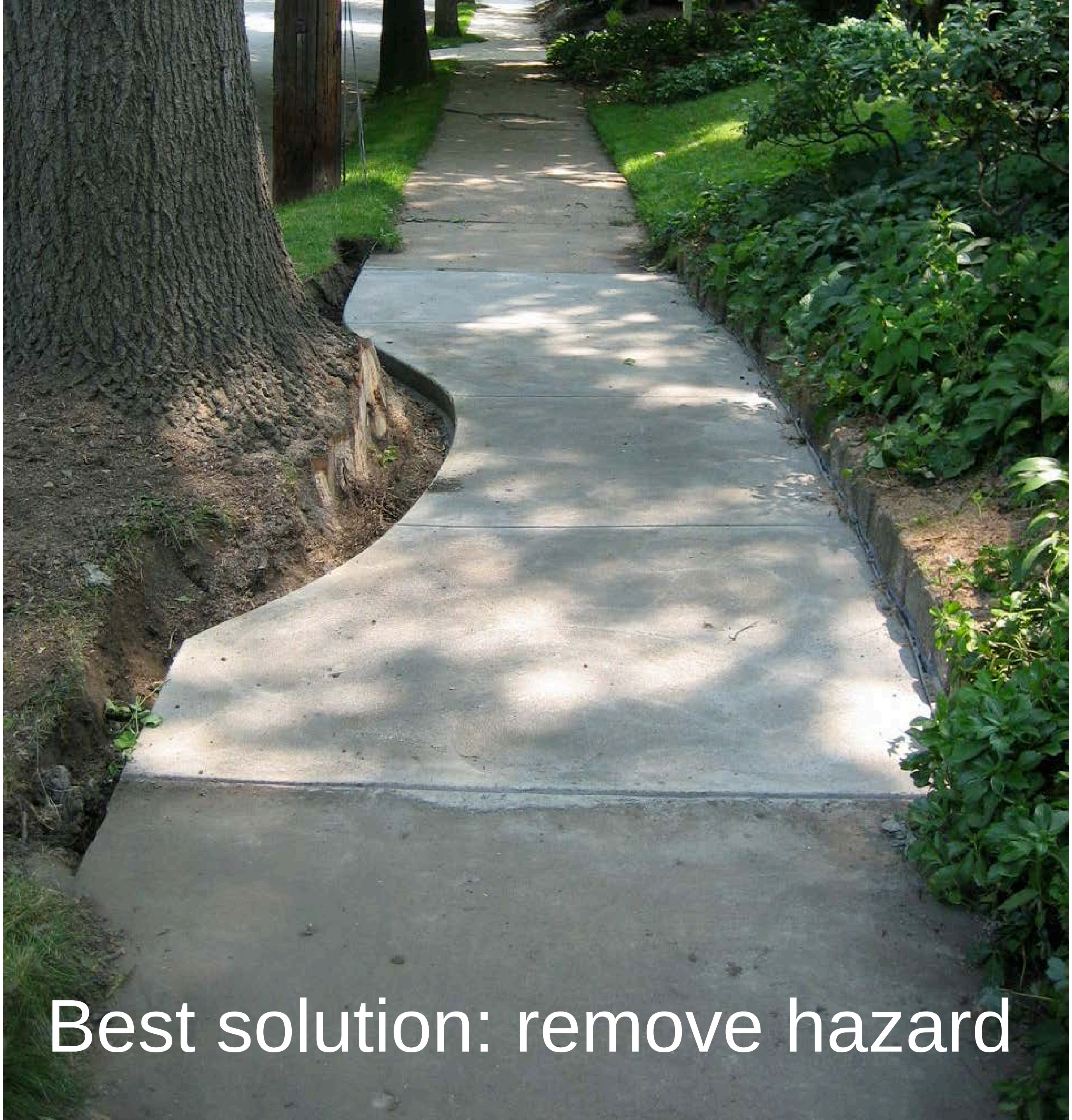
Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept lilliputian snotweasel foxtrot omegaforce.

Image courtesy of Johnathan Nightingale

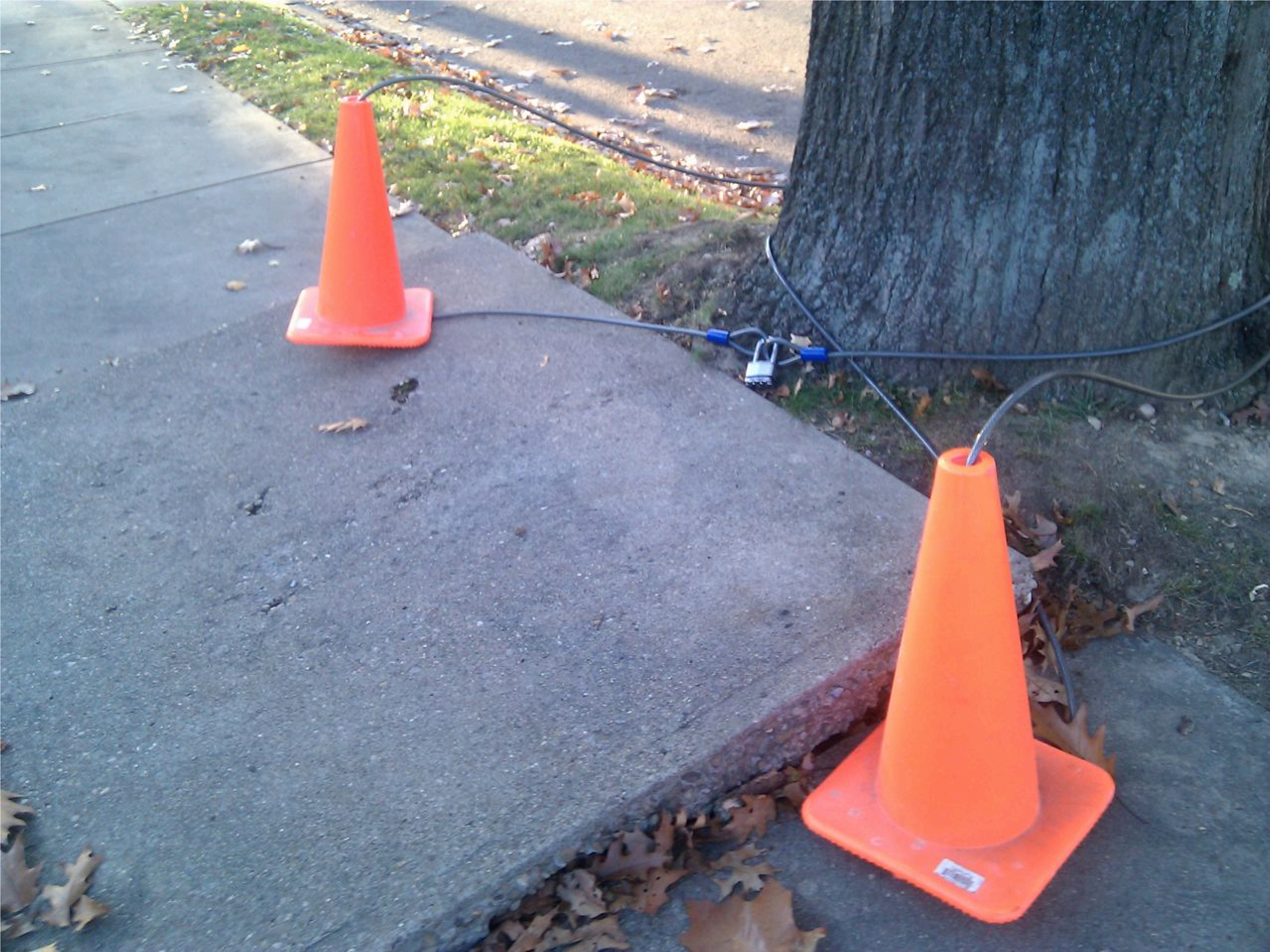


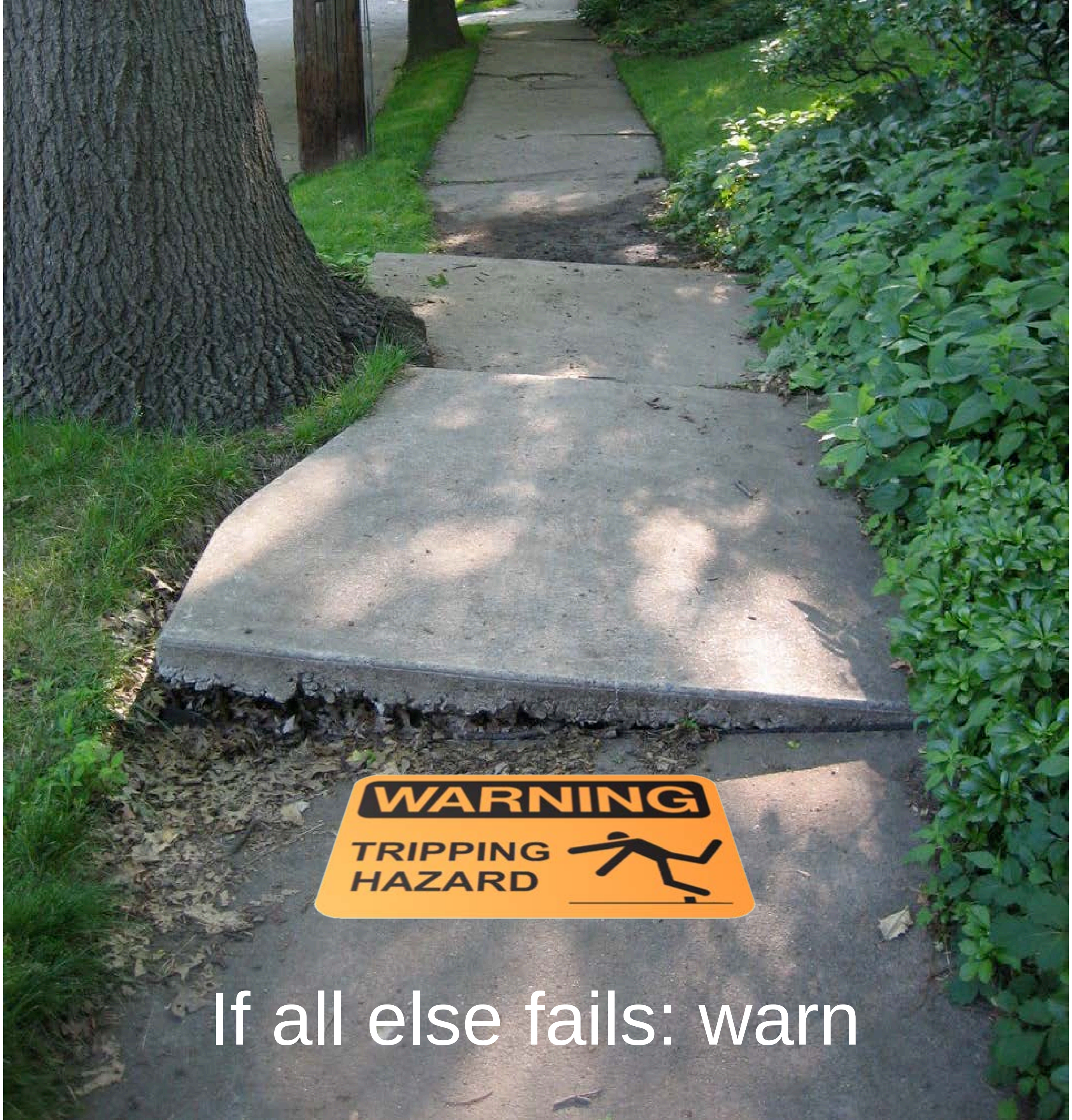
What to do about hazards?



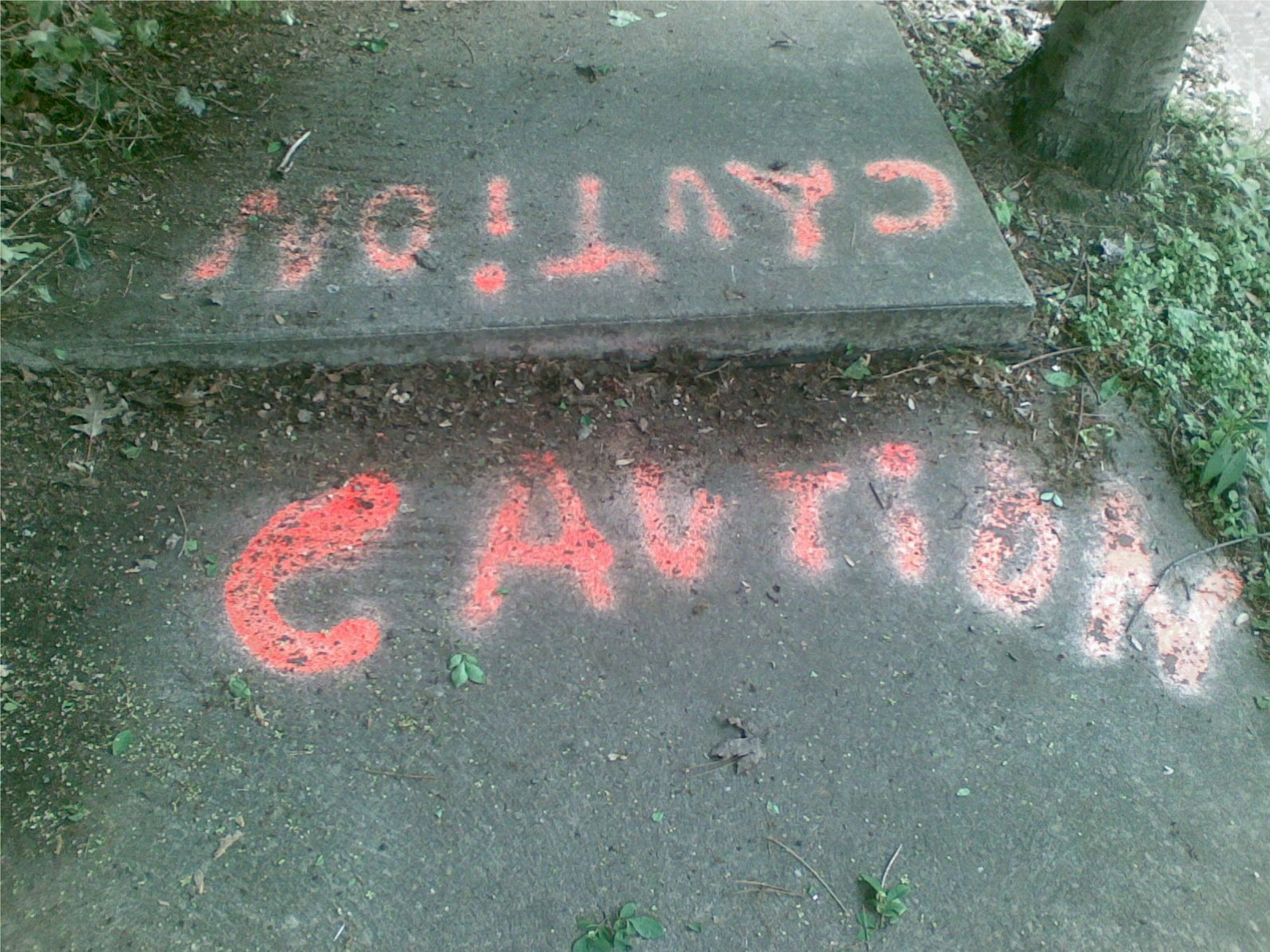
Best solution: remove hazard

Next best: guard against hazard

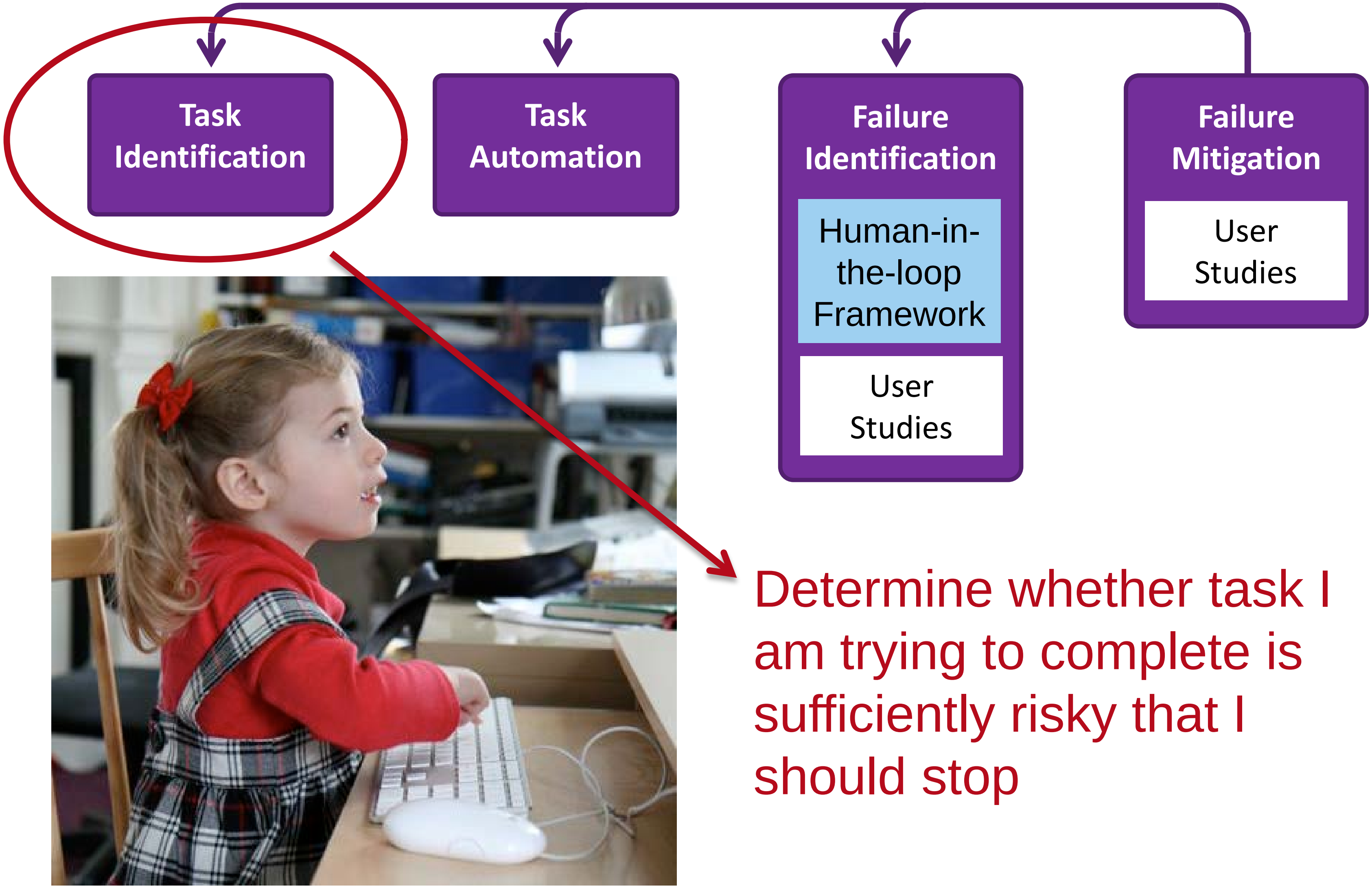




If all else fails: warn


CAUTION
CAUTION

Human threat mitigation for warnings



Task Identification

Task Automation

Failure Identification

Human-in-the-loop Framework

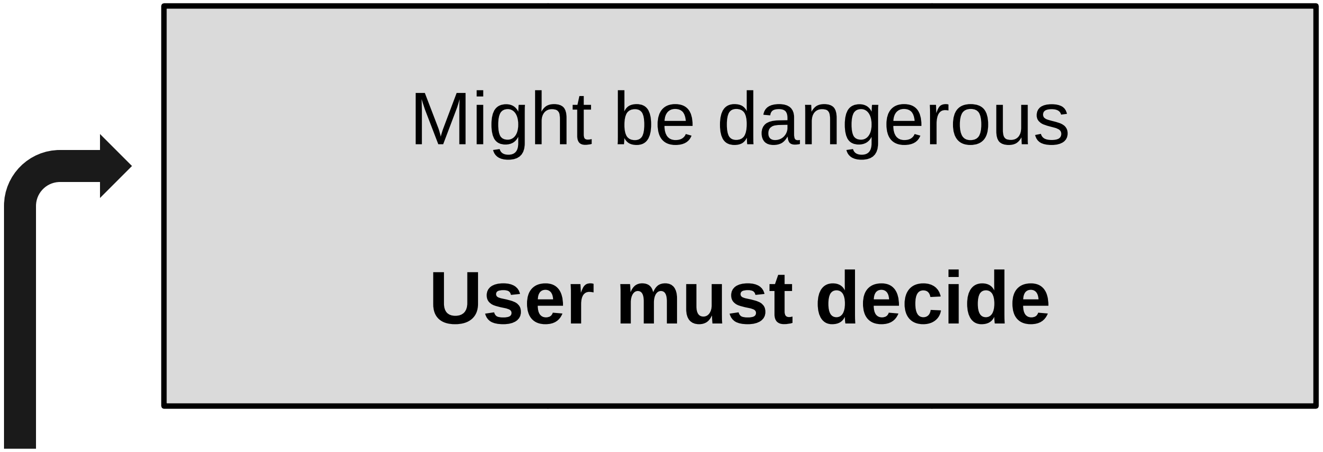
User Studies

Failure Mitigation

User Studies

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

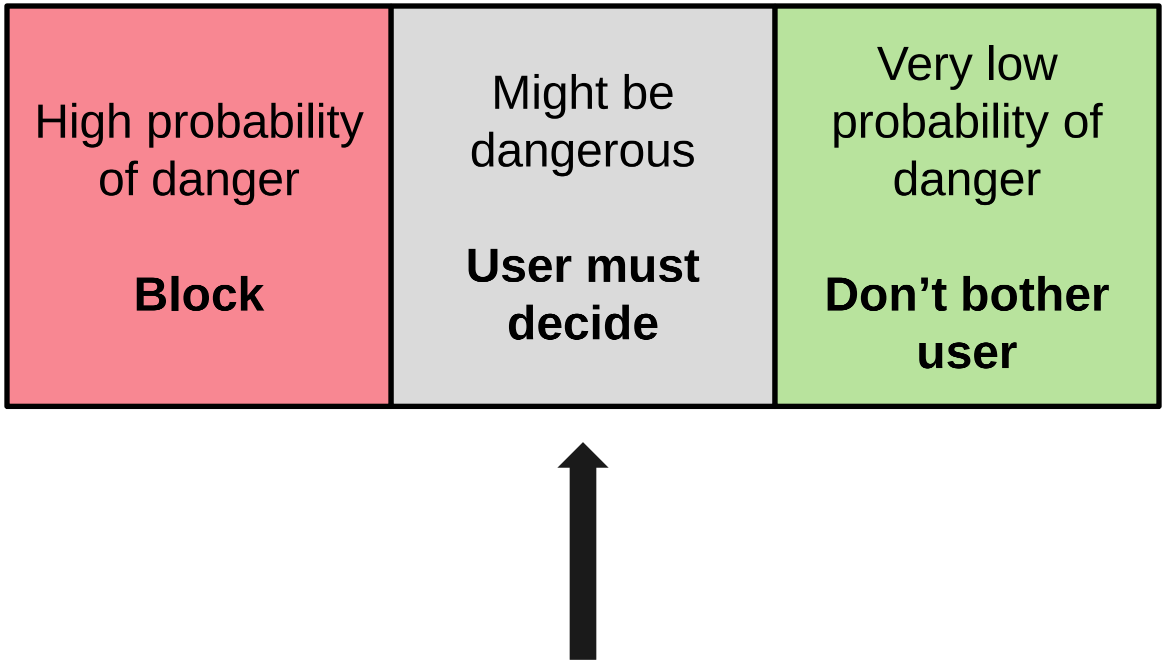


Might be dangerous

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?

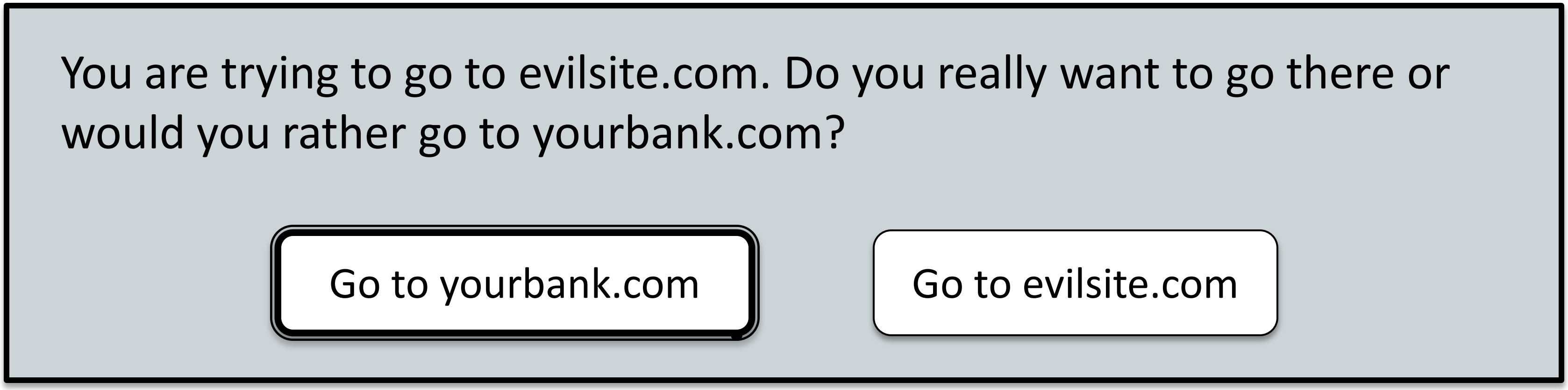
Don’t go there | Go there anyway

I don’t know what a phishing site is.

I really want to go to this site.

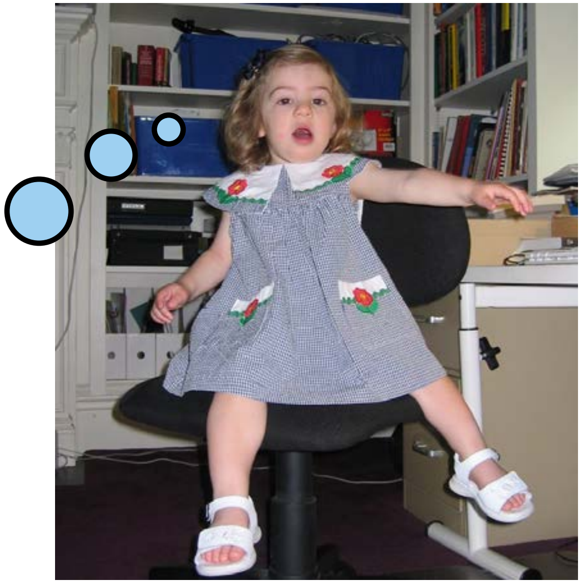
Of course I will go there anyway!

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?

Of course I want to go to yourbank.com!



Lorrie’s Trip last Thursday

Users are not the enemy!!!

Users are not the enemy

- “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 with 139 responses
  - 30 semi-structured interviews

Discussion points

- Are the participants representative?
  - Would a different group of participants produce different results?
- “Without feedback from security experts, users created their own rules on password design that were often anything but secure… many users do not understand how password cracking works.”
  - What feedback should we give?

Discussion points

- “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?
- Are shared passwords the solution?
- Are single-sign-on passwords the solution?