01. Course Overview; Introduction to Usable Security & Privacy

Blase Ur and Mainack Mondal

March 26th, 2018

CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO

Security, Usability, & Privacy Education & Research

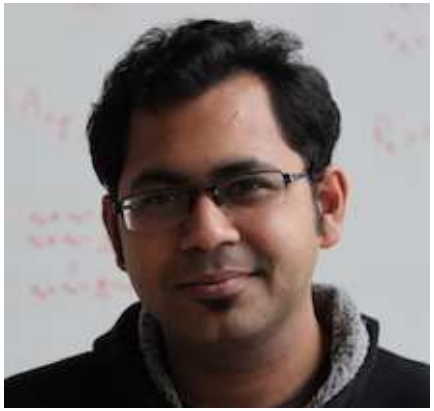
Today's class

- Course staff introductions
- Usable security and privacy = ???
- Course policies / syllabus
- Overview of course topics
- Usability / the human in the loop
- Current events

Introductions

- Blase Ur
- Assistant Professor of CS
  - Joined in January 2017
  - PhD at CMU in Fall 2016, advised by Lorrie Cranor
- SUPERgroup: Security, Usability, & Privacy Education & Research
- ~~"Professor Ur"~~ ~~"Dr. Ur"~~ "Blase" ~~"Dr. Blase"~~
- Office: Ryerson 157

Introductions



- Mainack Mondal
- Postdoctoral researcher
  - Joined in December 2017
  - PhD at MPI-SWS, advised by Krishna Gummadi
- Office: Young 4th floor

Introductions

- Weijia He
- Ph.D. student
  - Joined in Fall 2017
  - Advised by Blase Ur
- Office hour location: Young 4th floor

Introductions

- Ahsan Pervaiz
- Ph.D. student
  - Joined in Fall 2017
  - Advised by Blase Ur
- Office hour location: Young 4th floor

Humans

"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."

— C. Kaufman, R. Perlman, and M. Speciner
Network Security: PRIVATE Communication in a PUBLIC World.
2nd edition. Prentice Hall, page 237, 2002.

Security & Privacy

+

Human-Computer Interaction

=

Usable Security and Privacy

User-selected passwords

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

What makes usable security hard?

- Presence of an adversary
- Usability is not enough. We also need systems that remain secure when:
  - Attackers (try to) fool users
  - Users behave in predictable ways
  - Users are acting under stress
  - Users are careless, unmotivated, busy

Goals for this course

- Gain an appreciation for the importance of usability within security and privacy
- Learn about current research in usable security and privacy
- Learn how to conduct usability studies
- Learn how to critically examine user studies you hear about or read about

Course communication

- Updated syllabus is always available: https://super.cs.uchicago.edu/usable18/
- We will sign you up for Piazza
  - Opt in to get emails when we send announcements!

Components of your grade

- Quizzes (daily): 10%
- Midterm (take-home): 10%
- Final exam: 15%
- Problem sets (5): 25%
- Group Project: 40%

Required textbook

- There is no required textbook

Readings

- Generally one or two required readings per class
- Complete the readings before class
- Most readings from recent conferences
- 33210 students: about one additional reading per week

Quizzes

- Given in the first five minutes of class
- Will be a quick quiz based on that day's required reading
- If you will be unable to arrive on time for a class, submit a reading summary and highlight of the required reading(s) as a private post on Piazza
- Drop two lowest grades

Problem sets

- 5 problem sets
  - Submit them on Canvas
  - No late problem sets accepted!
- 33210 only: “reading summary”
  - 3-7 sentence summary
  - One “highlight”

What are problem sets like?

- Conduct mini studies + report results
- Evaluate the incidence or state of something in the real world
- Write code that sheds some insight on usable security and privacy
- Conduct usability evaluations of tools
- Propose possible studies

Example reading summary

Ur et al. investigated whether crowdsourced recommendations impact the Firefox privacy settings humans and sloths choose. They conducted a 183-participant lab study in which participants were prompted to set up a clean installation of Firefox as they normally would when given a new computer. Participants were randomly selected either to see crowdsourced recommendations for the settings, or no recommendations. They found that both humans and sloths were statistically significantly more likely to choose privacy-protective settings when given recommendations, though sloths took 83 times as long to do so.

Highlight: I wonder if the results would have differed if they had used Chrome, rather than Firefox. Chrome's privacy settings are hidden behind multiple browser clicks. I would be surprised if Chrome recommendations change non-use of privacy settings.

Exams

- Take-home “midterm” (like a problem set) due April 23rd
- Closed-book final during exam period
- These will ask you to use the skills developed in class, rather than remembering trivia
- Prepare by doing the readings and participating in discussions

Project

- Design, conduct, and analyze a pilot user study in usable privacy or security
  - Groups assigned based on your preferences
  - We will provide a list of project topics but your suggestions are welcome
- Deliverables: Project proposal, ethics application, progress report & presentation, final paper, and final presentation (May 23rd)

Participation in class

- You are expected to participate in class
  - Raise your hand during discussions
  - Share interesting news on Piazza
  - Play an active role in small-group activities
  - Spark discussion on Piazza
- You are expected to be in class (on time!)
- Please note exam and group presentation dates and DO NOT schedule job interviews on those dates

23210 vs. 33210

- Same lectures
- Same* assignments
  - 33210 students have extra problems
- Same project
  - 33210 students must have implementation

23210 vs. 33210

- 23210 is an elective within UG CS major
- 33210 may count for UG programming languages and systems sequence if you successfully petition
- Graduate students must take 33210
  - Systems elective

Academic integrity

- University of Chicago policies about plagiarism and academic integrity
- Don’t look at other students’ assignments
  - Exception: When we explicitly say you may
  - Talking verbally about problem sets is ok
- Quote text and cite ideas that are not yours
- Consequences of cheating and plagiarism range from a 0 on the assignment to expulsion from the University of Chicago

Wellness

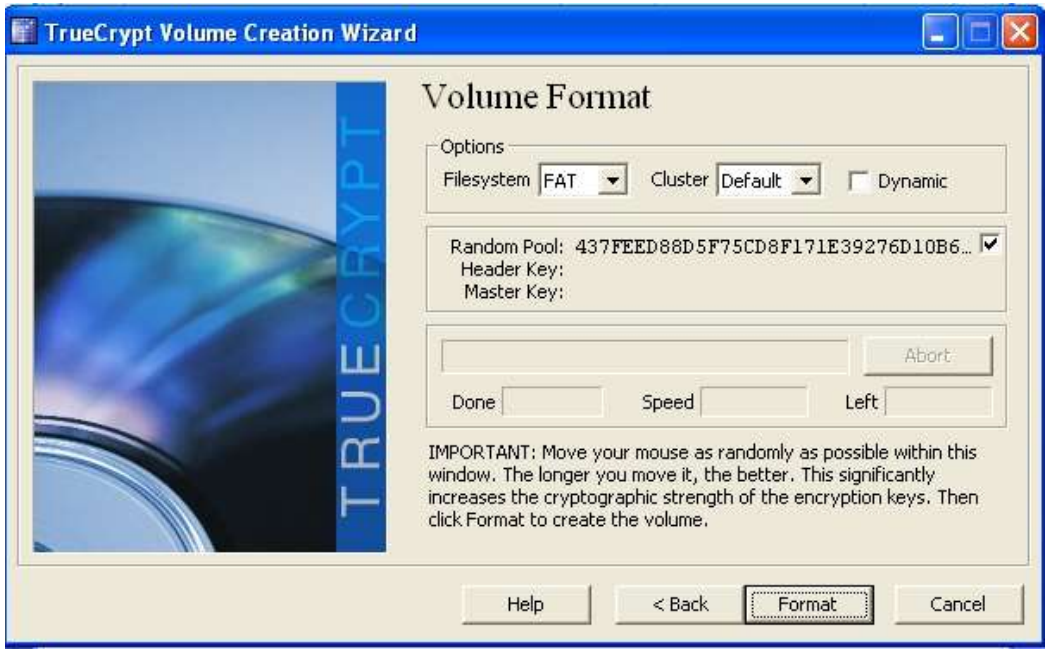
- Take care of yourself during the class
- Let us know if you are overwhelmed
- Take advantage of the university's wellness and mental health resources

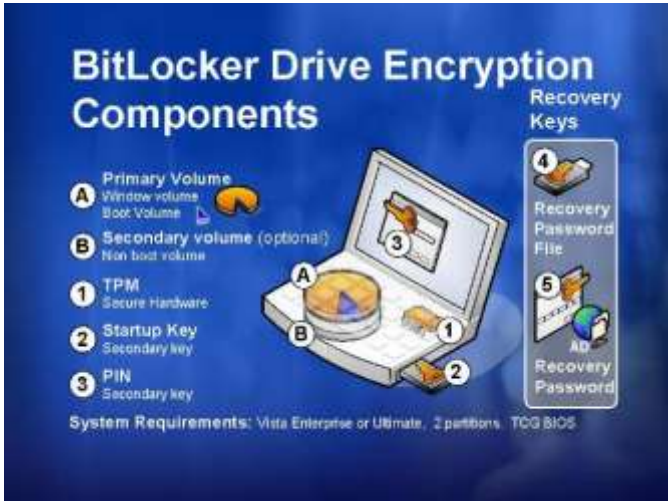
Course topics

- Overviews of security and privacy
- Introduction to HCI methods and the design of experiments
  - How (and why) to conduct different types of quantitative and qualitative studies
  - Ecological validity and ethics
- Specific usable privacy and security topics

Usable encryption

- Why don't people encrypt their email and their files?





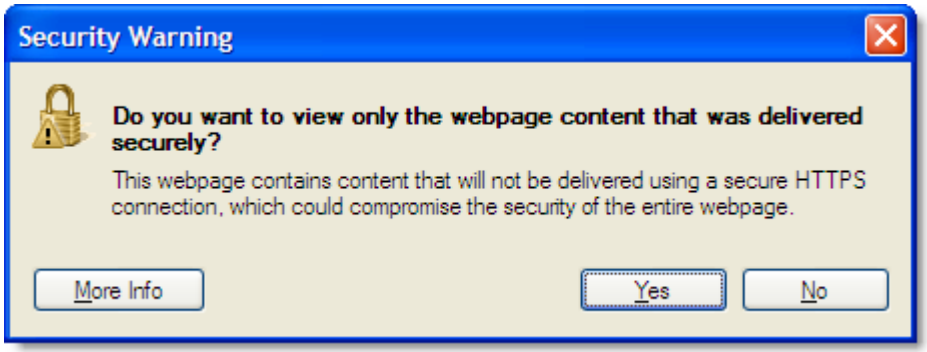
Passwords

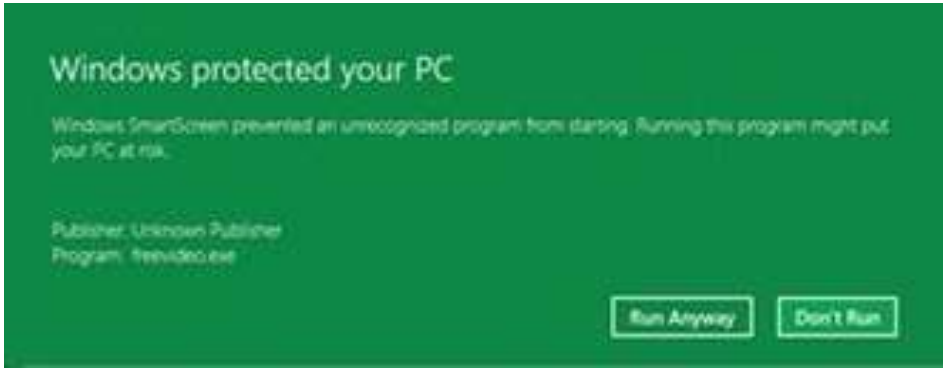
- Can people make passwords that are easy to remember, yet hard to crack?

Password strength: Poor. Consider adding a digit or making your password longer.

Security warnings

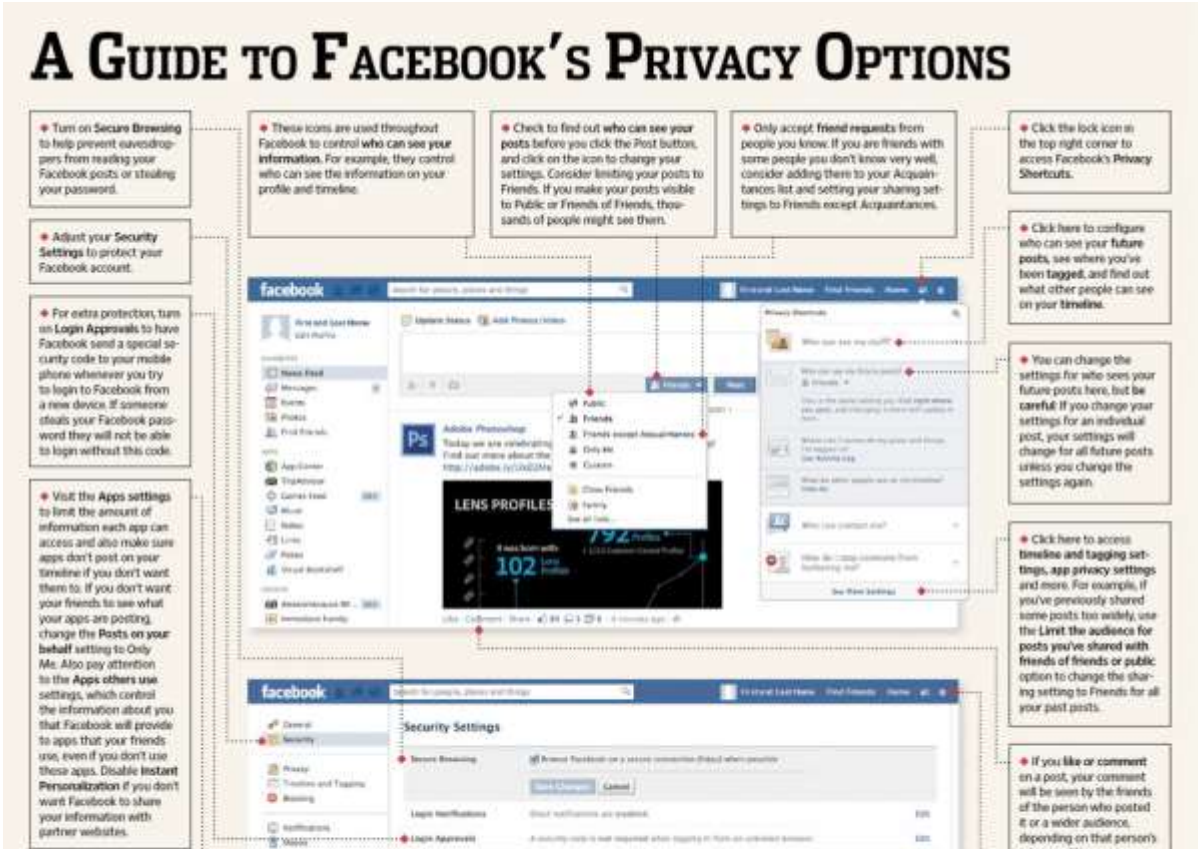
- Can we make them more effective?

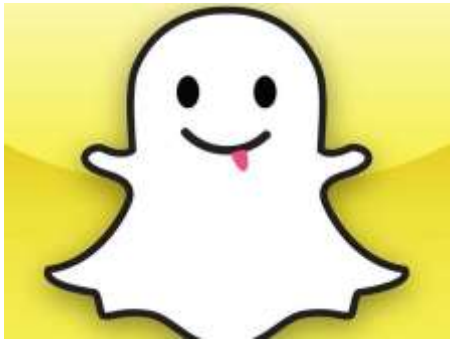




Social media and privacy

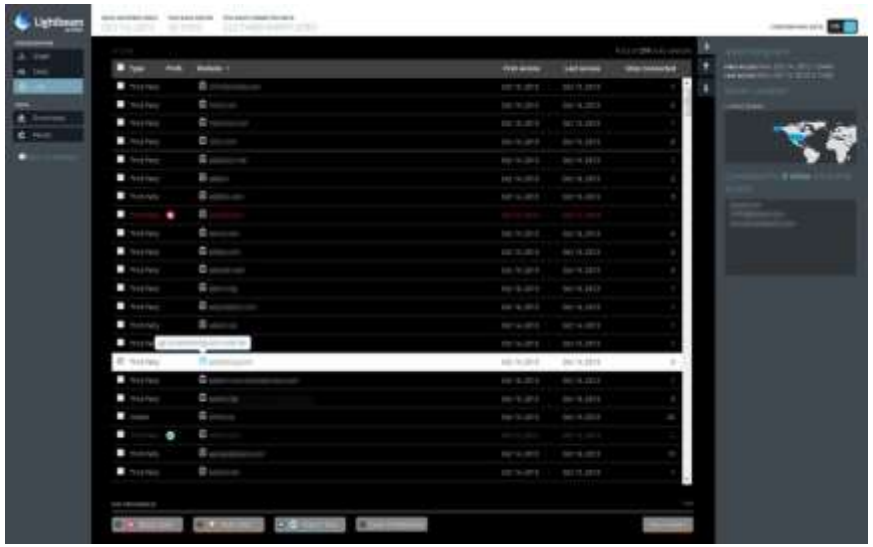
- Can people want to share some things widely, yet want other things to be private?





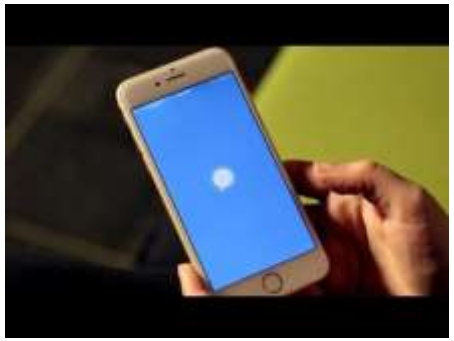
Web security & privacy

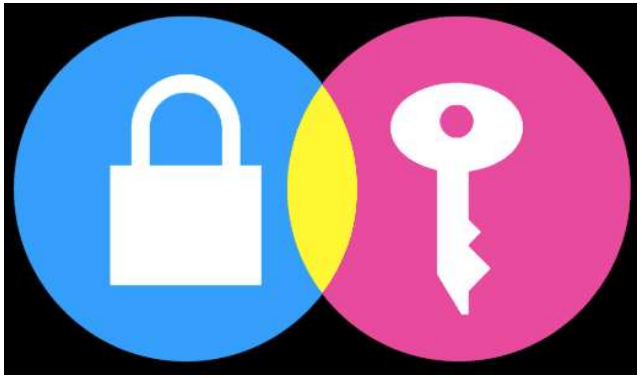
- How do we keep the web secure and private, and how do we keep users aware of what's happening as they browse?



Anonymity; activists/journalists

- Can anonymity tools help journalists, activists, and others protect their privacy?





Privacy notice and choice

- How do we communicate privacy-critical information in a sea of information?

SoundCloud Class B

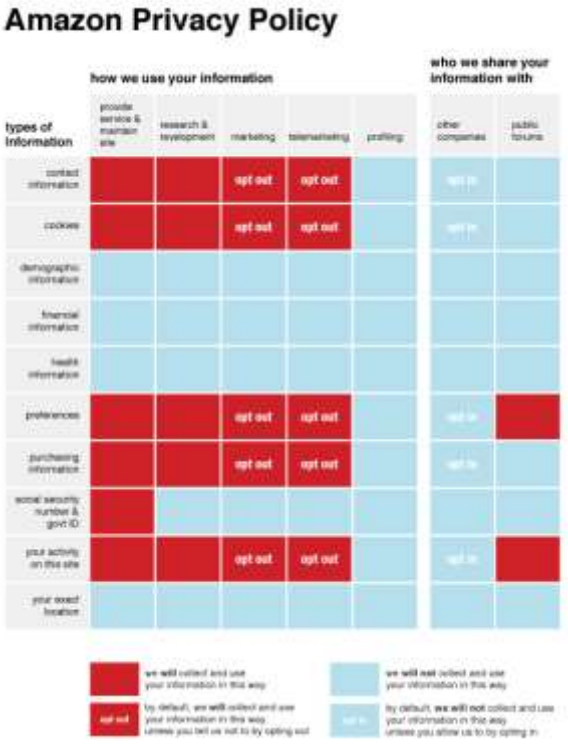
- You stay in control of your copyright
- Collected personal data used for limited purposes
- 6 weeks to review changes
- Indemnification from claims related to your content or your account
- Personal information can be disclosed in case of business transfer or insolvency

More details

Rev. 12/2010

FACTS WHAT DOES **FARMERS-MERCHANTS BANK (FM Bank)** DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and **Income** ■ **Account balances** and **Payment History** ■ **Credit history** and **Credit scores** When you are *no longer* our customer, we continue to share your information as described in this notice.



Mobile devices and the IoT

- What are the privacy and security implications of new ways of computing?

Mental models; anti-phishing

- How do non-technical people think about privacy and security, and how can we better support them?

Developers are users, too

- How can we make security and privacy usable for the experts who are building your tools?

Inclusive security & privacy

- How can we design security and privacy to work for everyone?
  - Age
  - Abilities
  - Culture

Fair & accountable machine learning

- How can we verify that automated systems relevant to security and privacy are fair, accountable, and transparent?

The Human in the Loop

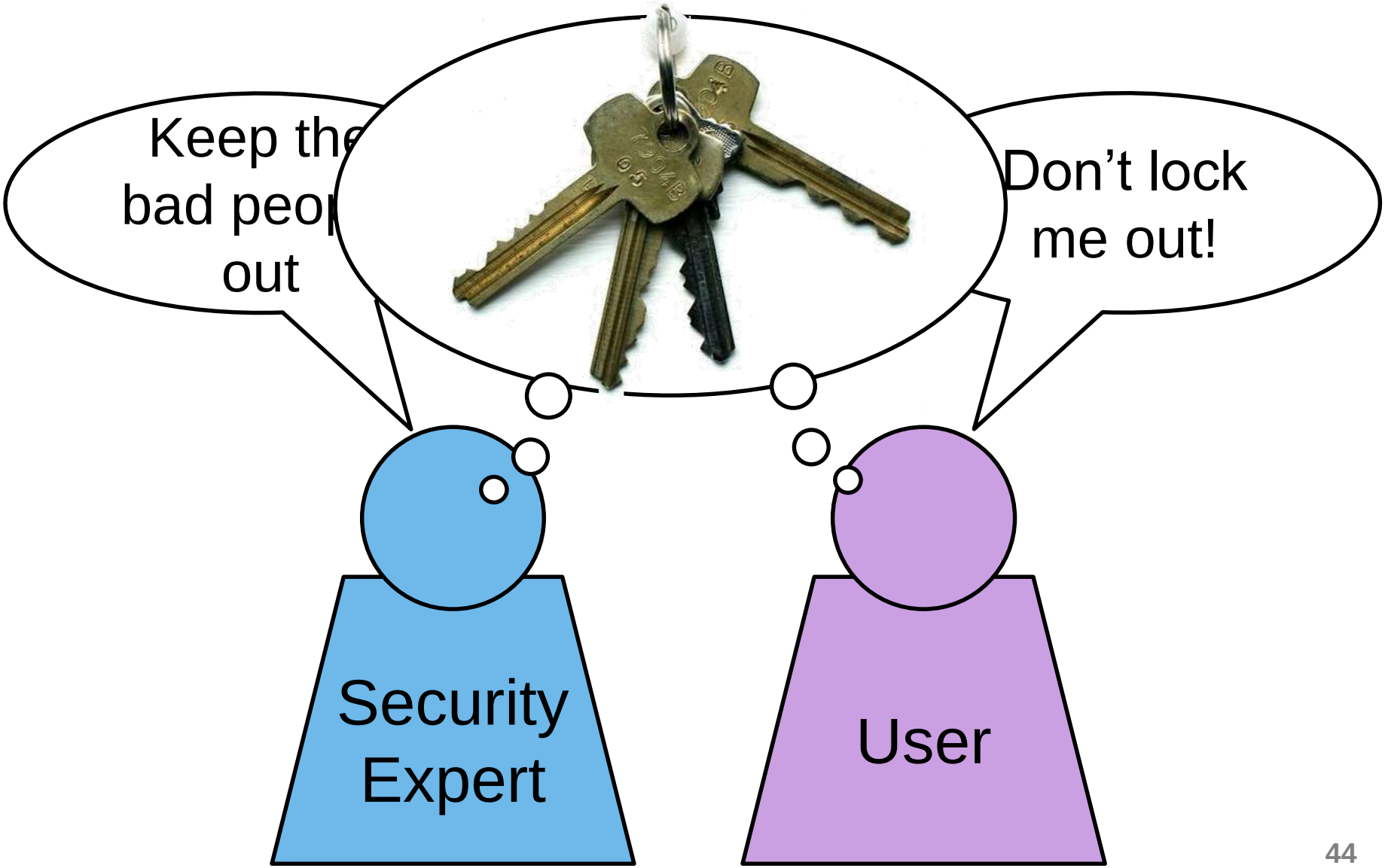
The human threat

- Malicious humans
- Clueless humans
- Unmotivated humans
- Humans constrained by human limitations

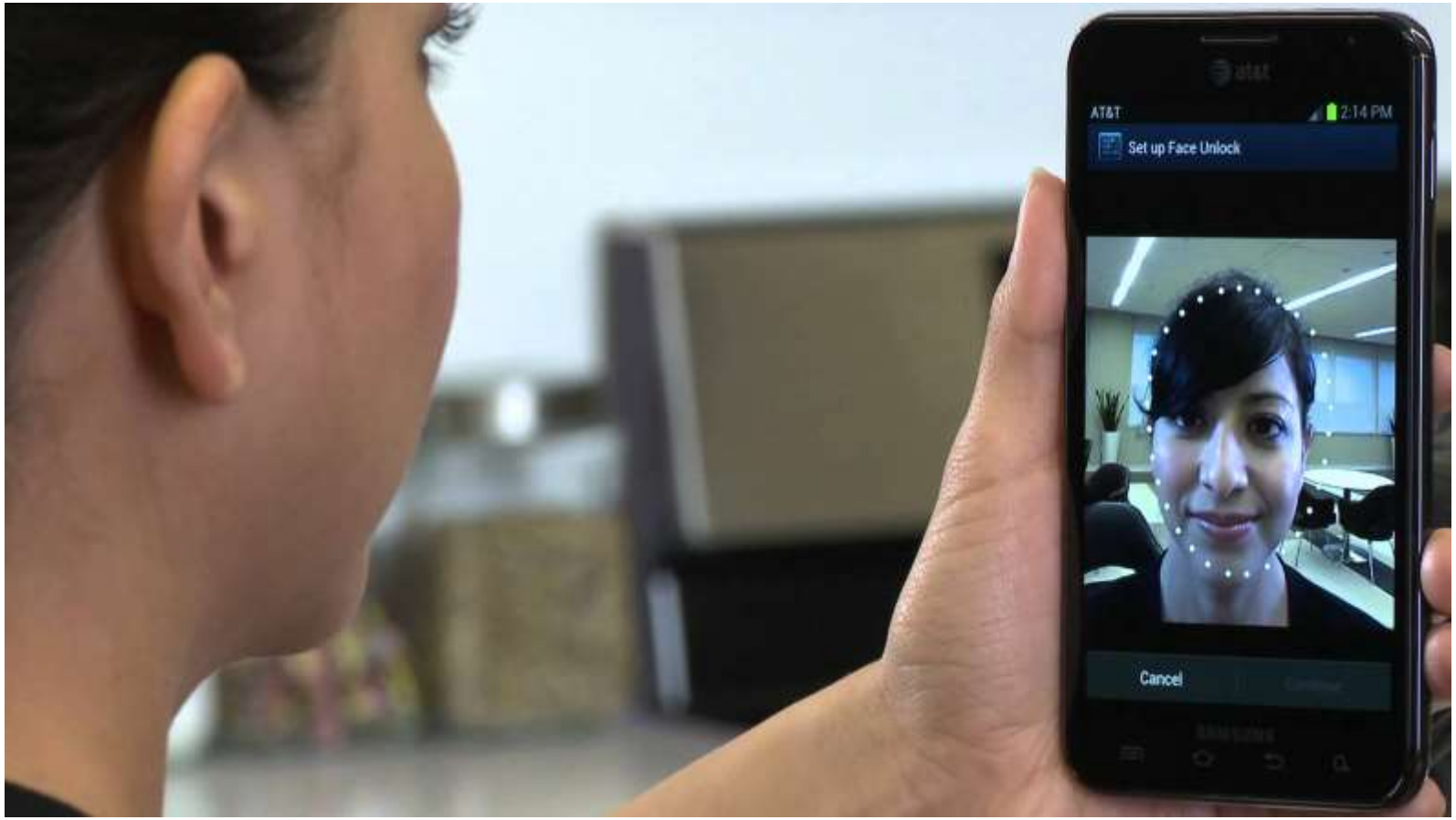
Are you capable of remembering a different strong password for every account you have?

Security is a secondary task

Concerns may not be aligned

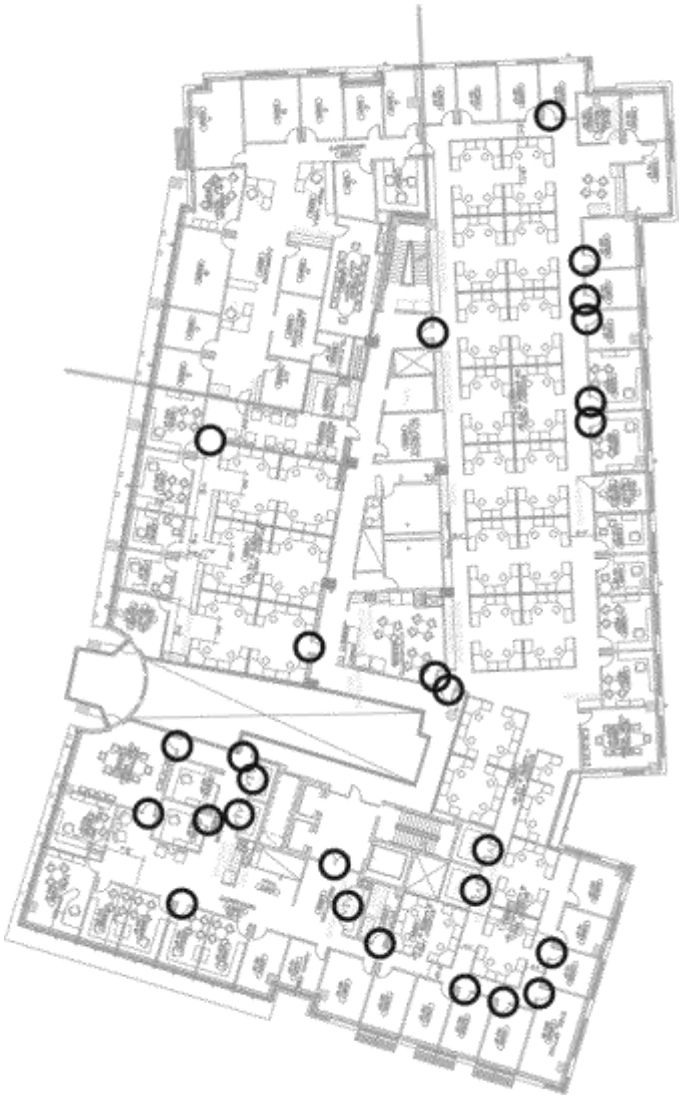


Perceptions have an important impact



Perceptions have an important impact

Perceptions have an important impact



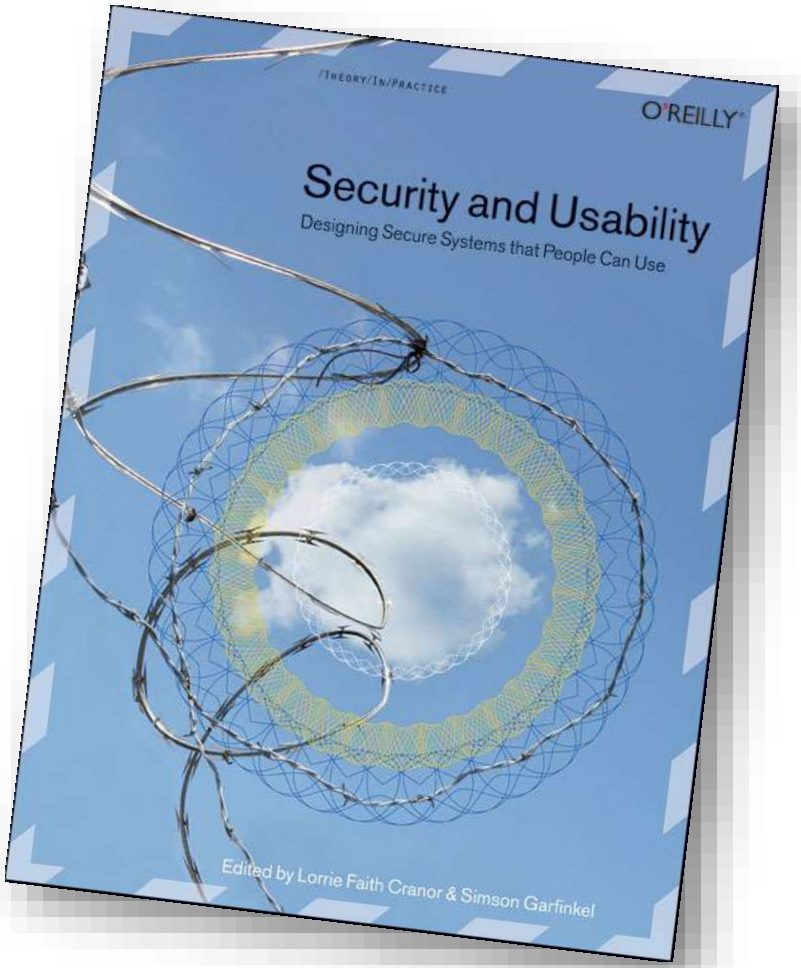
Perceptions have an important impact

"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."

Convenience always wins

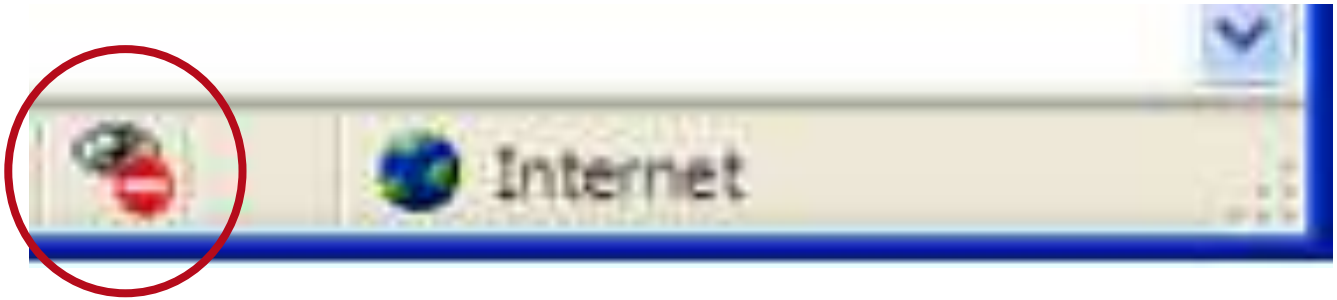
How can we make secure systems more usable?

- 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



Visual communication


TM


Internet

What can make a system unusable?

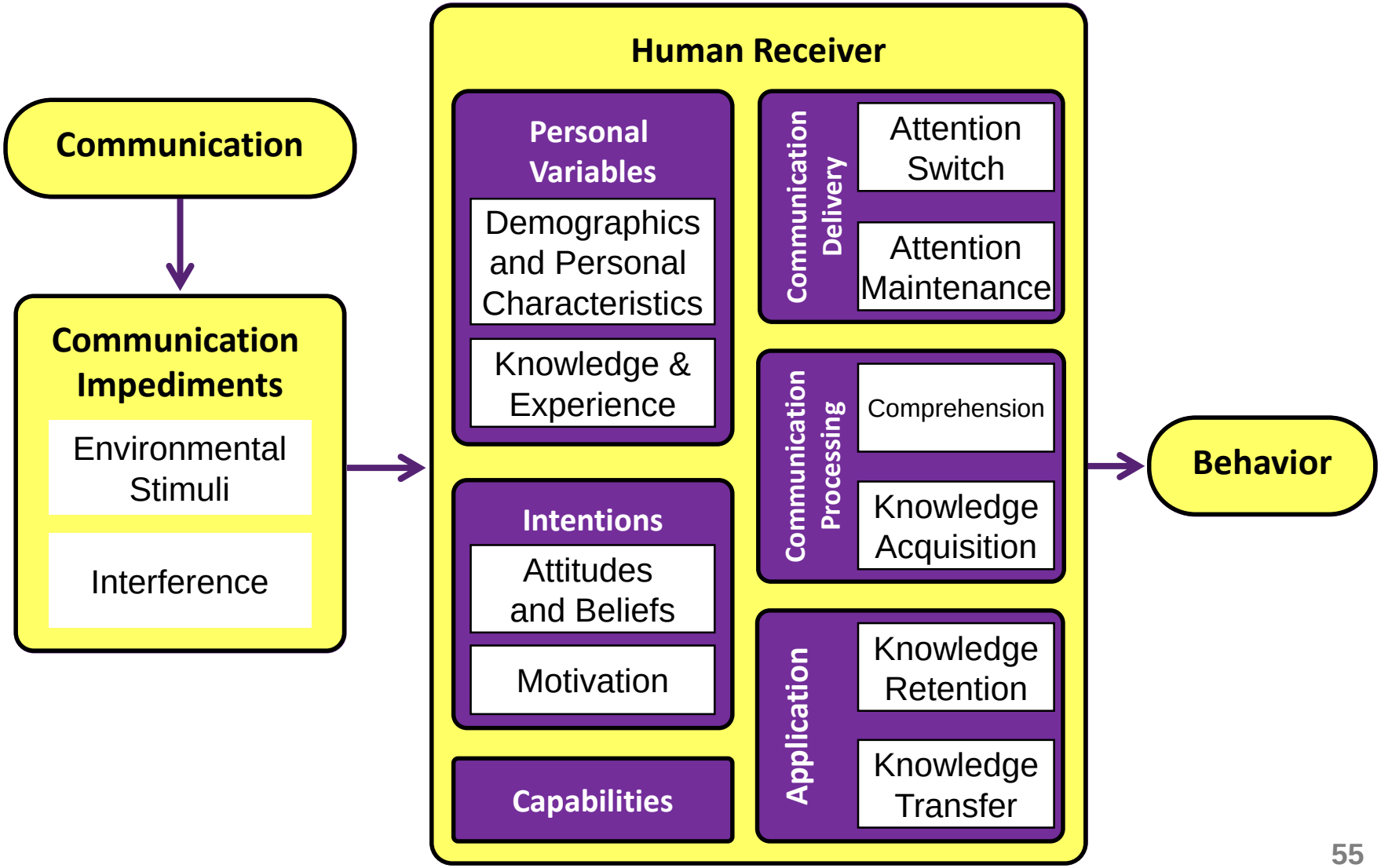
- Confusing / misleading / unhelpful user interface
- Requiring a user to make decisions for which the user is not qualified
- Assuming knowledge or abilities that the user doesn’t have
- Assuming unreasonable amount of attention / effort

Human-in-the-loop framework

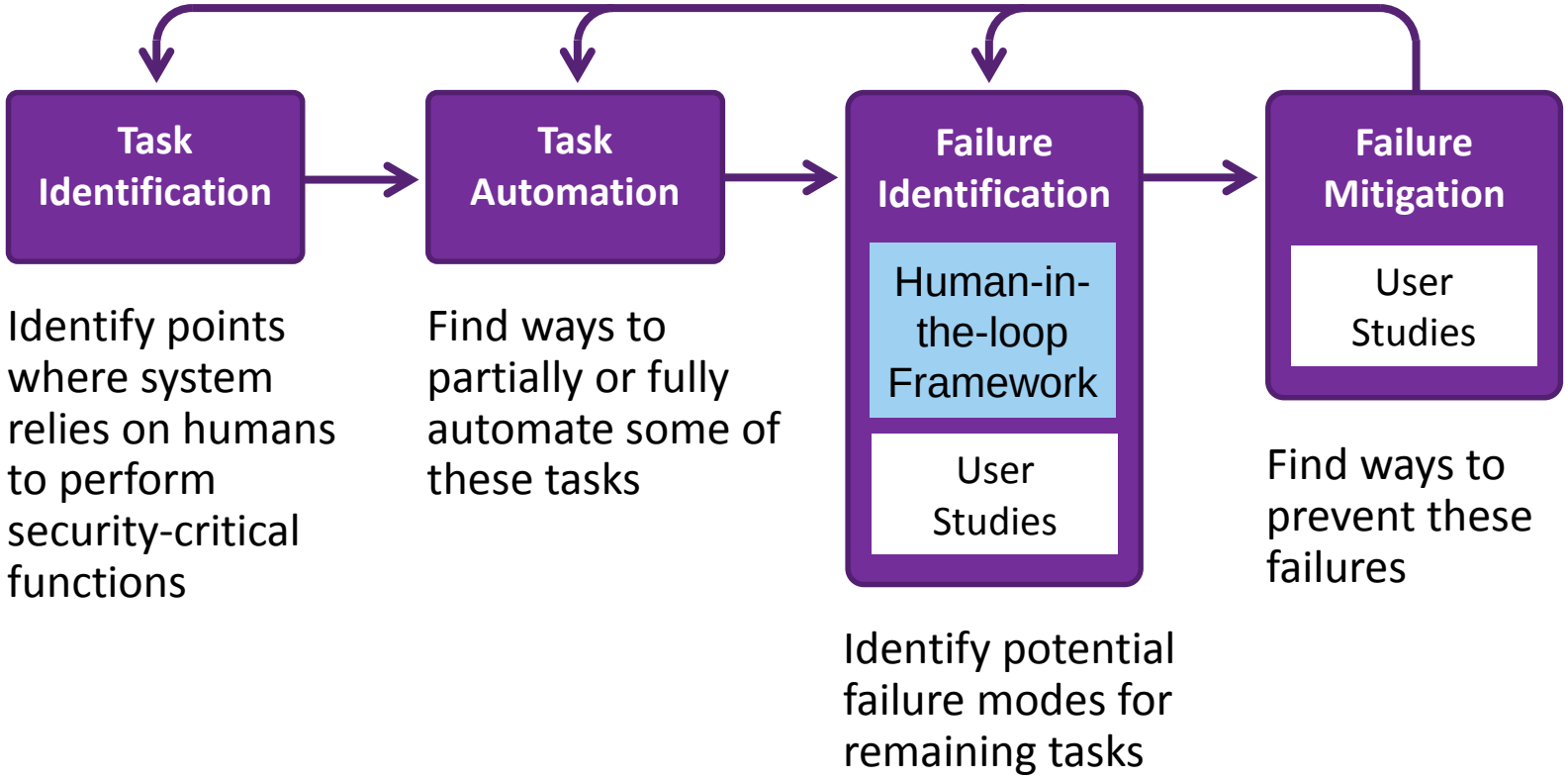
- Based on Communication-Human Information Processing Model (C-HIP) from Warnings Science
- Models human interaction with secure systems
- Can help identify human threats

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



Threat identification & mitigation



Understand human 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?

Designing for Usability

What to do about hazards?

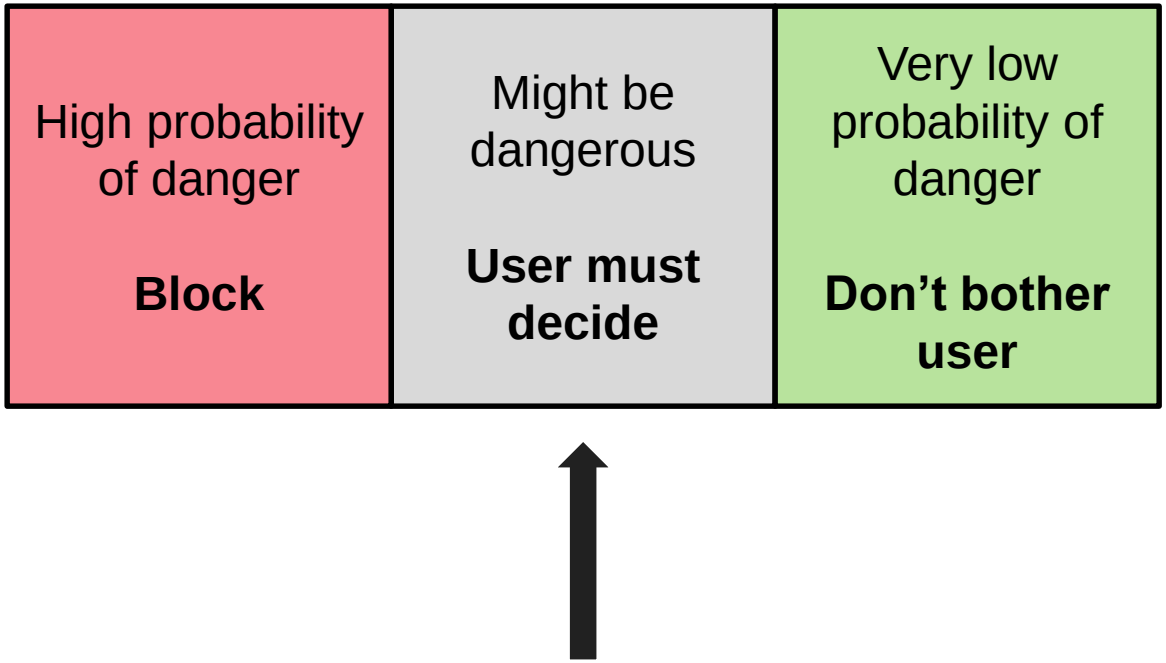

Best solution: remove hazard

If all else fails: warn

A better solution would be to add a spring so the door won’t slam


HOLE

Support users' decisions



Help user decide by asking question user is qualified to answer

Image courtesy of Johnathan Nightingale

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


CREDIT CARD
ONLY
DEBIT CARD
ONLY
Cash Only
VISA
Pay with cash or credit
CANCEL
NO
YES
NO CASH
ACCEPTED

People were confused until they posted instructions

Design communicates function

How do you unplug the sink?

How do you turn on this shower?

Stove layout

Stove layout

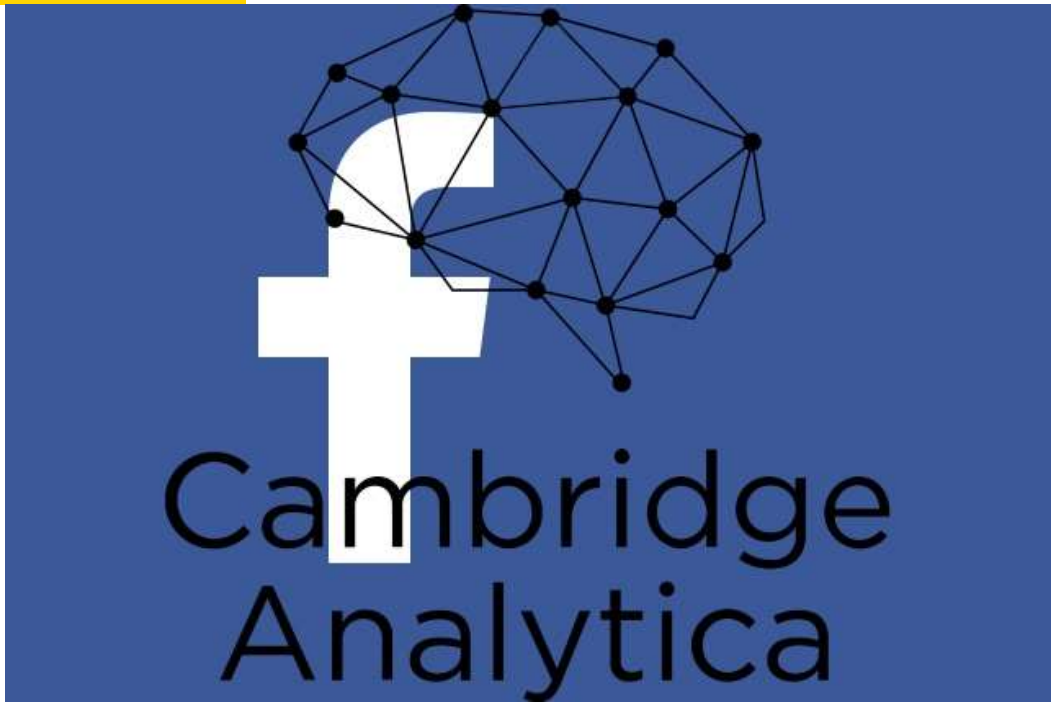
Stove layout

Doors

Doors

Doors

Cambridge
Analytica



Cambridge
Analytica