01. Course Overview; Introduction to Usable Security & Privacy

Blase Ur, March 27th, 2017
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
- Reasoning about the human in the loop

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”~~
- OH: Thursdays 1:00 – 2:00, Ryerson 157
  - This week: Friday 1:00 – 2:00

Introductions (TA staff)

- Maria Hyun
  - OH: Wednesdays 1:00 – 2:00, Ryerson 254
- Gushu Li
  - OH: Mondays 4:30 – 5:30, Ryerson 254
- Hua Li
  - OH: Fridays 3:00 – 4:00, Ryerson 375

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.

Interdisciplinary approach useful

Other disciplines have experience studying human behavior. We can borrow their models and methods:

- Psychology
- Sociology
- Cognitive sciences
- Warnings science
- Risk perception
- Behavioral economics
- HCI
- Design
- Communication
- Persuasive technology
- Learning science
- Network analytics

What makes usable security different?

- 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

Usable security research bridges security and usability

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?

Course communication

- Updated syllabus is always available: https://super.cs.uchicago.edu/usable17/
- We will sign you up for Piazza
  - Opt in to get emails when we send announcements!

Components of your grade

- Quizzes (daily): 16%
- Midterms (2): 20%
- Problem sets (5): 24%
- Group Project: 40%

Readings

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

Required textbook

- There is no required textbook

Quizzes

- Given in the first five minutes of class
  - End at 3:05 pm
- Will be a quick quiz based on that day’s required reading
- If you will be unable to arrive on time for a class, email a reading summary and highlight of the required reading(s) before class to the TAs

Problem sets

- 5 problem sets
  - Submit them printed, on paper!
  - No late problem sets accepted!
  - Drop single lowest grade
- 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
- 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.

“Midterms”

- Take-home “midterm” (like a problem set) due April 24th
- In-class “midterm” on May 22nd
- These will ask you to use the skills developed in class, rather than remembering trivia
- Prepare by doing the readings and participating in discussions

Final exam

- There is no final exam

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 31st)
- Submit a poster to SOUPS 2017 and/or a paper to another conference

Projects from prior UPS courses

- How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation (USENIX Security ‘12)
- The Post that Wasn't: Exploring Self-Censorship on Facebook (CSCW ‘13)
- QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks (USEC ‘13)
- Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption" (USEC '15)
- Supporting Privacy-Conscious App Update Decisions with User Reviews (SPSM ‘15)
- Usability and Security of Text Passwords on Mobile Devices (CHI ‘16)

Participation in class

- You are expected to participate in class
  - Raise your hand during discussions
  - Share interesting privacy/security news
  - Play an active role in small-group activities
  - Spark discussion on the class email list
- 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

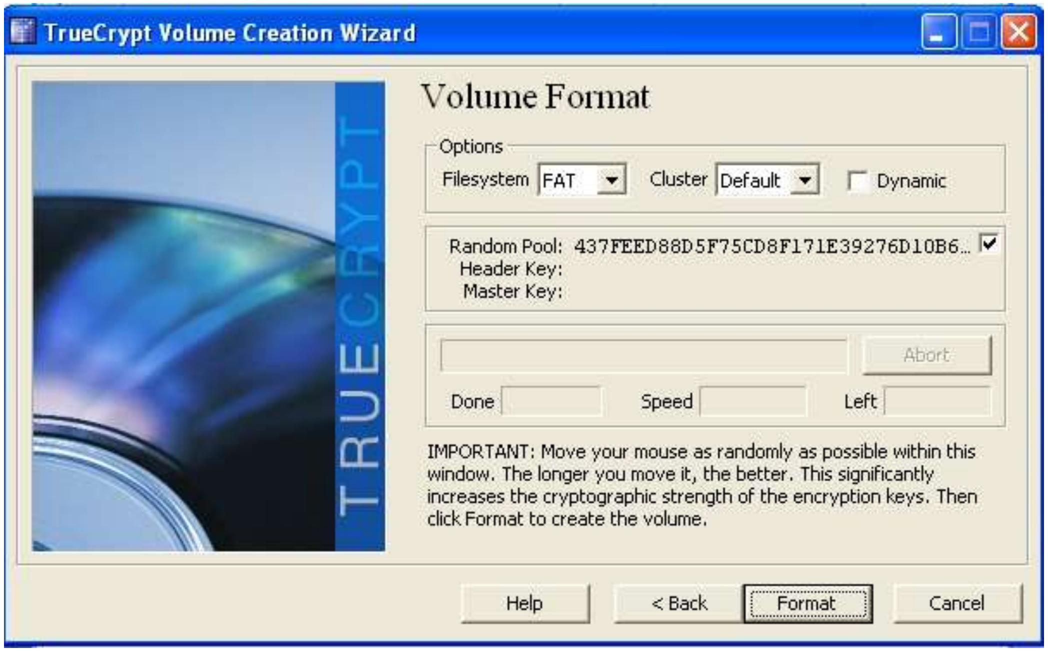
Course topics

- 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 (3/29)

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

GnuPG



TrueCrypt Volume Creation Wizard

Volume Format

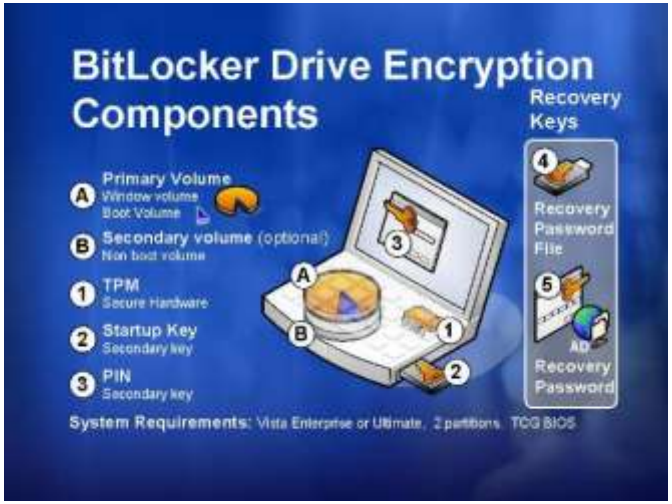
Options

Filesystem FAT ▾ Cluster Default ▾ ☐ Dynamic

Random Pool: 437FEED88D5F75CD8F171E39276D10B6... ☑
Header Key:
Master Key:

Done Speed Left

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.



BitLocker Drive Encryption Components

Ⓐ Primary Volume
Window volume
Boot Volume

Ⓑ Secondary volume (optional)
Non boot volume

① TPM
Secure Hardware

② Startup Key
Secondary key

③ PIN
Secondary key

Recovery Keys

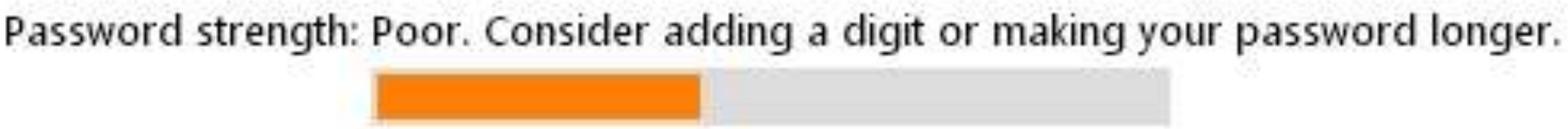
④ Recovery Password File

⑤ AD Recovery Password

System Requirements: Vista Enterprise or Ultimate, 2 partitions, TCG BIOS

Passwords (4/5)

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

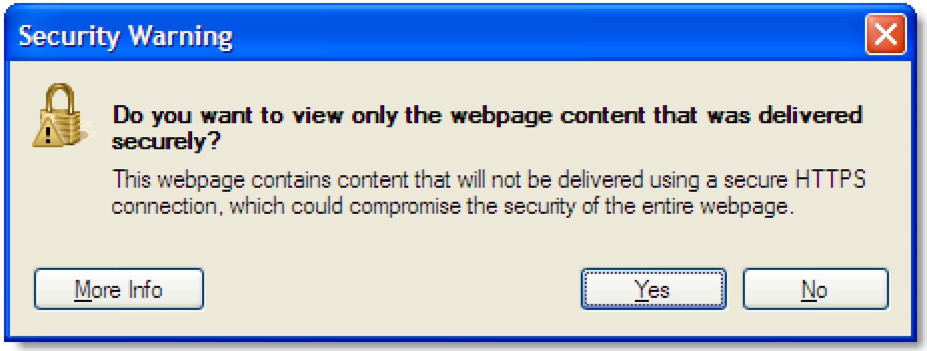


Password strength: Poor. Consider adding a digit or making your password longer.

password
123456789
iloveyou
princess
rockyou
12345678
abc123
nicole
tigger
michael
purple
liverpool
soccer
flower
ashley
daniel
password1
andrea
tinkerbell
lovely
qwerty
jordan
football
angels
justin
pretty
chelsea
secret
barbie
andrew
playboy
666666
jasmine
butterfly
basketball
softball
matthew
shadow
melissa
christian
elizabeth
brandon
poohbear
anthony
jesus
mickey
hello
1234567890

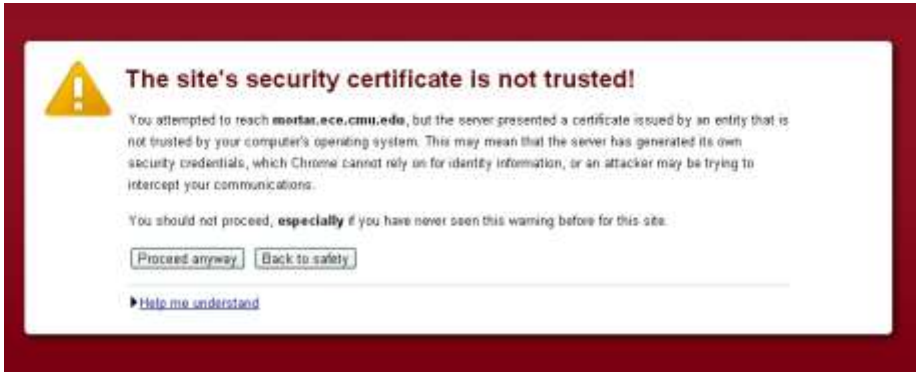
Security warnings (4/12)

- Can we make them more effective?



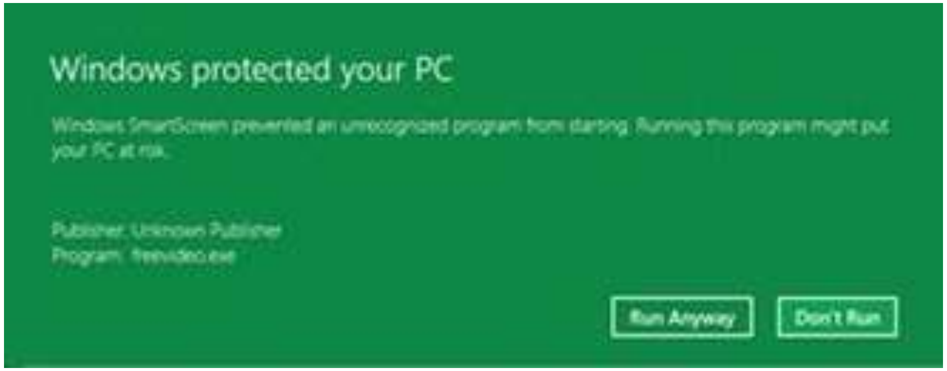
Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.


The site's security certificate is not trusted!

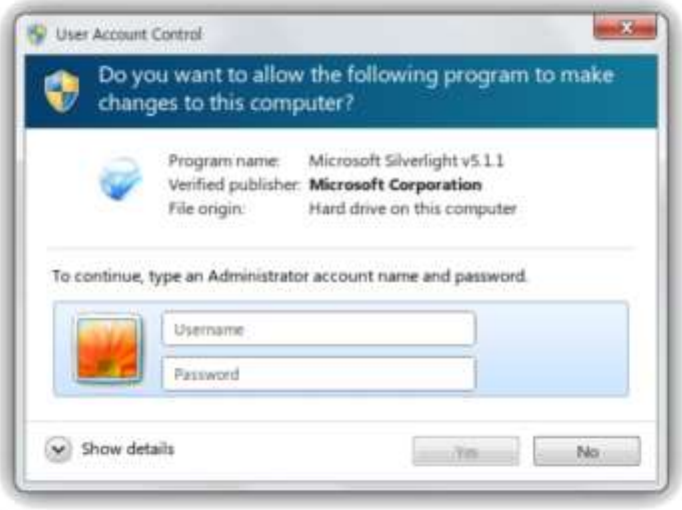
You attempted to reach **mortar.ece.cmu.edu**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.


Windows protected your PC

Windows SmartScreen prevented an unrecognized program from starting. Running this program might put your PC at risk.

Publisher: Unknown Publisher
Program: freevideo.exe



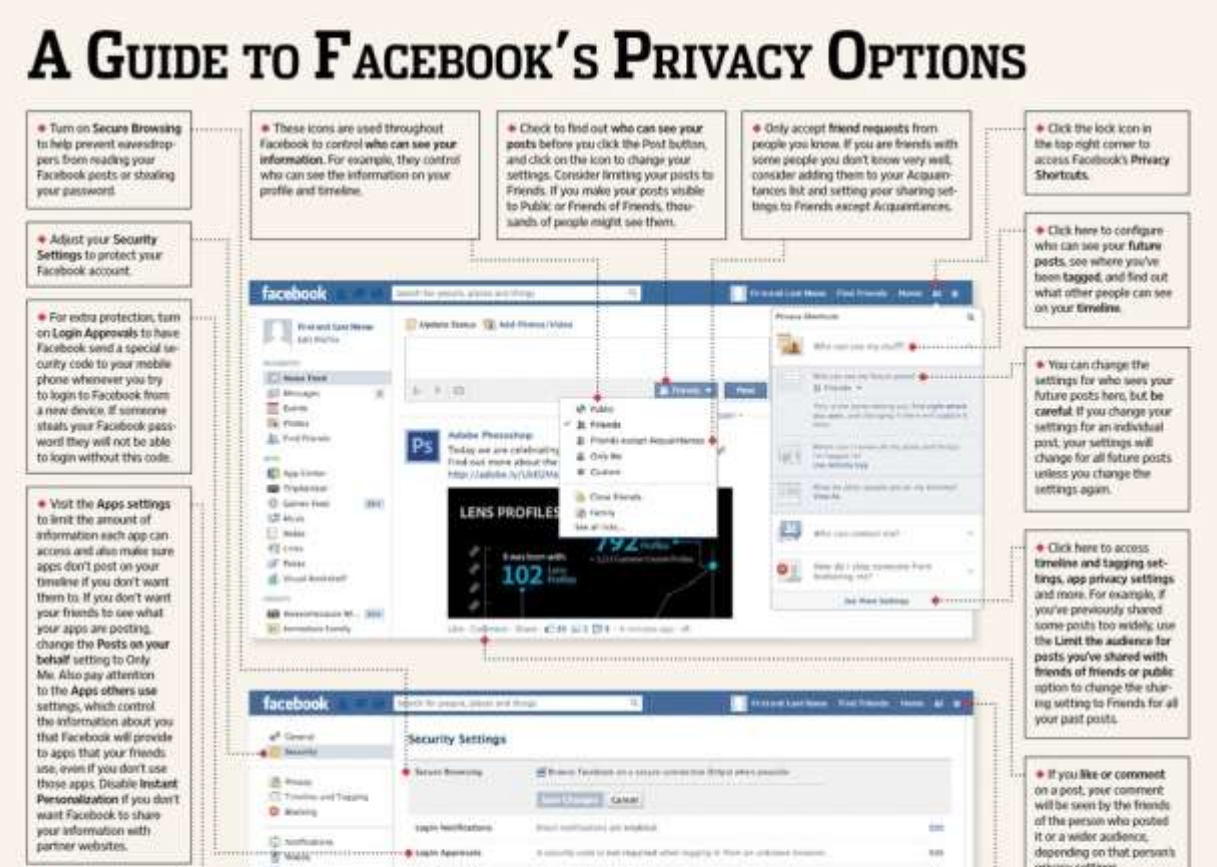
Do you want to allow the following program to make changes to this computer?

Program name: Microsoft Silverlight v5.1.1
Verified publisher: **Microsoft Corporation**
File origin: Hard drive on this computer

To continue, type an Administrator account name and password.

Social media and privacy (4/17)

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



A Guide to Facebook's Privacy Options

- Turn on **Secure Browsing** to help prevent eavesdroppers from reading your Facebook posts or stealing your password.
- Adjust your **Security Settings** to protect your Facebook account.
- For extra protection, turn on **Login Approvals** to have Facebook send a special security code to your mobile phone whenever you try to login to Facebook from a new device. If someone steals your Facebook password they will not be able to login without this code.
- Visit the **Apps settings** to limit the amount of information each app can access and also make sure apps don't post on your timeline if you don't want them to. If you don't want your friends to see what your apps are posting, change the **Posts on your behalf** setting to Only Me. Also pay attention to the **Apps others use** settings, which control the information about you that Facebook will provide to apps that your friends use, even if you don't use those apps. Disable **Instant Personalization** if you don't want Facebook to share your information with partner websites.
- These icons are used throughout Facebook to control **who can see your information.** For example, they control who can see the information on your profile and timeline.
- Check to find out **who can see your posts** before you click the Post button, and click on the icon to change your settings. Consider limiting your posts to Friends. If you make your posts visible to Public or Friends of Friends, thousands of people might see them.
- Only accept **friend requests** from people you know. If you are friends with some people you don't know very well, consider adding them to your Acquaintances list and setting your sharing settings to Friends except Acquaintances.
- Click the lock icon in the top right corner to access Facebook's **Privacy Shortcuts.**
- Click here to configure who can see your **future posts**, see where you've been **tagged**, and find out what other people can see on your **timeline**.
- You can change the settings for who sees your future posts here, but **be careful**. If you change your settings for an individual post, your settings will change for all future posts unless you change the settings again.
- Click here to access **timeline and tagging settings, app privacy settings** and more. For example, if you've previously shared some posts too widely, use the **Limit the audience for posts you've shared with friends of friends or public** option to change the sharing setting to Friends for all your past posts.
- If you **like or comment** on a post, your comment will be seen by the friends of the person who posted it or a wider audience, depending on that person's

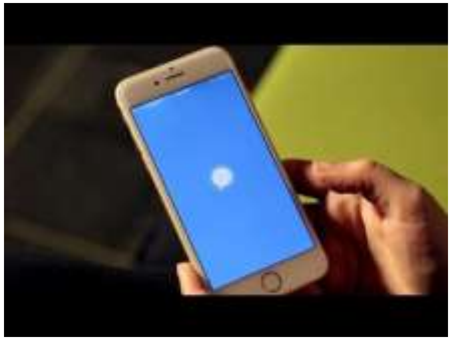
Web security & privacy (4/24)

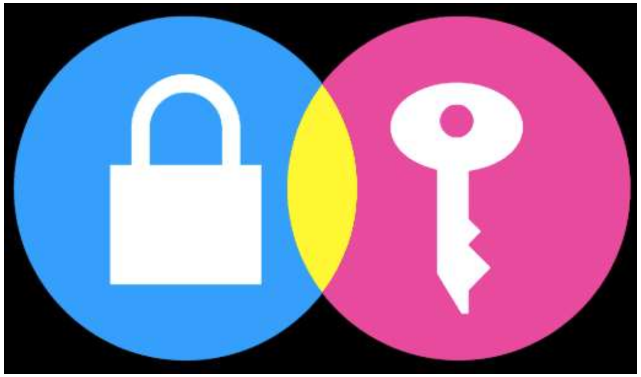
- How do we keep the web secure and private, and how do we keep users aware of what's happening as they browse?

AdChoices

Anonymity; activists/journalists (4/26)

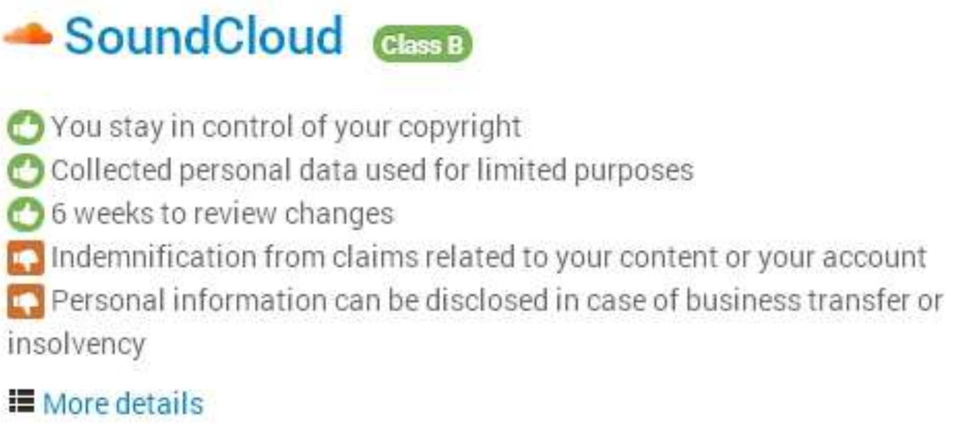
- Can anonymity tools help journalists, activists, and others protect their privacy?





Privacy notice and choice (5/1)

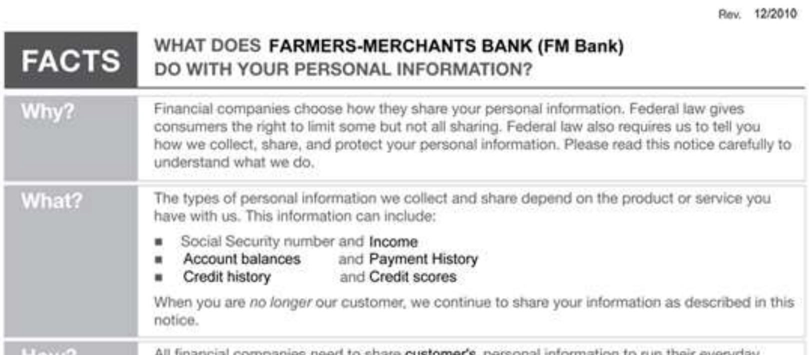
- How do we communicate privacy-critical information in a sea of information?



SoundCloud Class B

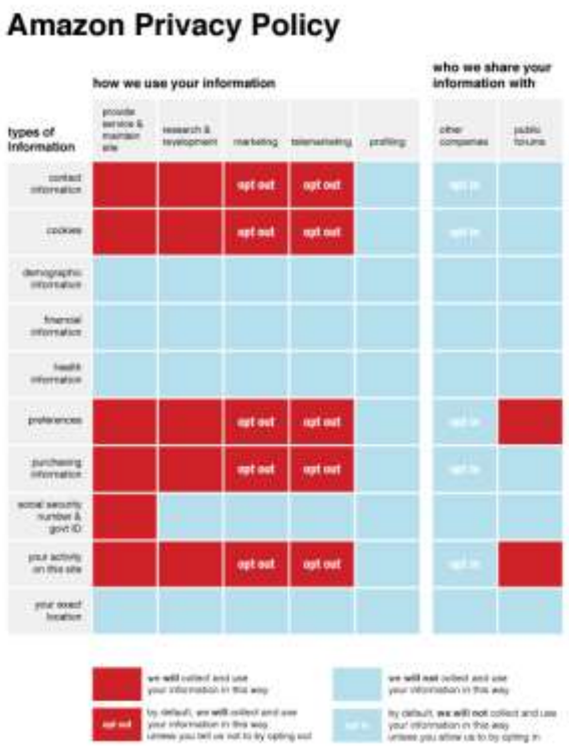
- 👍 You stay in control of your copyright
- 👍 Collected personal data used for limited purposes
- 👍 6 weeks to review changes
- 👎 Indemnification from claims related to your content or your account
- 👎 Personal information can be disclosed in case of business transfer or insolvency

☰ 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.
How?	All financial companies need to share **customer's** personal information to run their everyday



Amazon Privacy Policy

types of information	how we use your information: provide service & maintain site	research & development	marketing	telemarketing	profiling	who we share your information with: other companies	public forums
contact information	🟥	🟥	opt out	opt out	🟦	opt in	🟦
cookies	🟥	🟥	opt out	opt out	🟦	opt in	🟦
demographic information	🟦	🟦	🟦	🟦	🟦	🟦	🟦
financial information	🟦	🟦	🟦	🟦	🟦	🟦	🟦
health information	🟦	🟦	🟦	🟦	🟦	🟦	🟦
preferences	🟥	🟥	opt out	opt out	🟦	opt in	🟥
purchasing information	🟥	🟥	opt out	opt out	🟦	opt in	🟦
social security number & govt ID	🟥	🟦	🟦	🟦	🟦	🟦	🟦
your activity on this site	🟥	🟥	opt out	opt out	🟦	opt in	🟥
your exact location	🟦	🟦	🟦	🟦	🟦	🟦	🟦

🟥 **we will** collect and use your information in this way

🟦 **we will not** collect and use your information in this way

🟥 opt out: by default, **we will** collect and use your information in this way unless you tell us not to by opting out

🟦 opt in: by default, **we will not** collect and use your information in this way unless you allow us to by opting in

Mobile devices and the IoT (5/3)

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

Mental models; user education (5/15)

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

Developers are users! (5/17)

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

stackoverflow

GitHub

Inclusive security & privacy (5/24)

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

The Human in the Loop

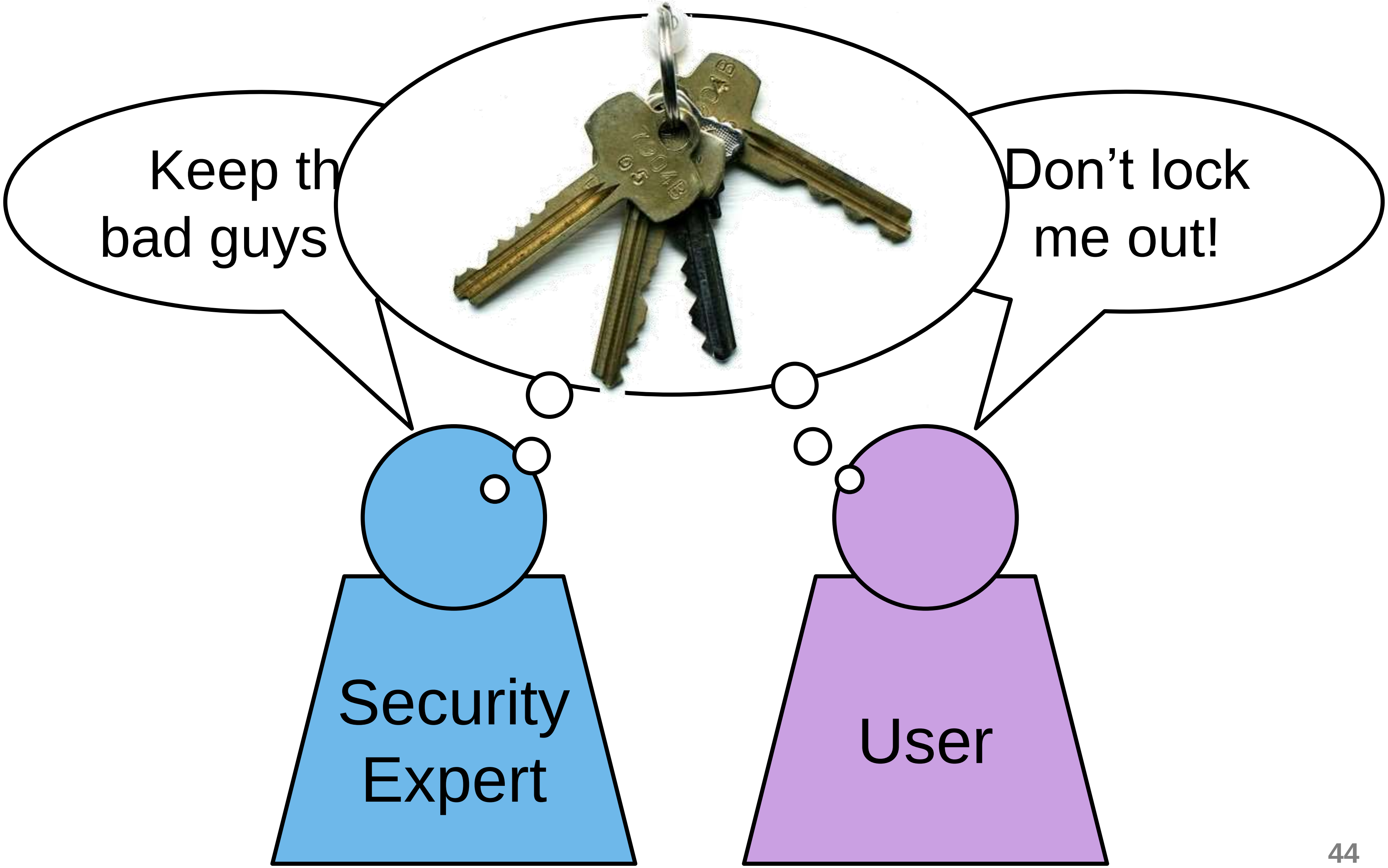
The human threat

- 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



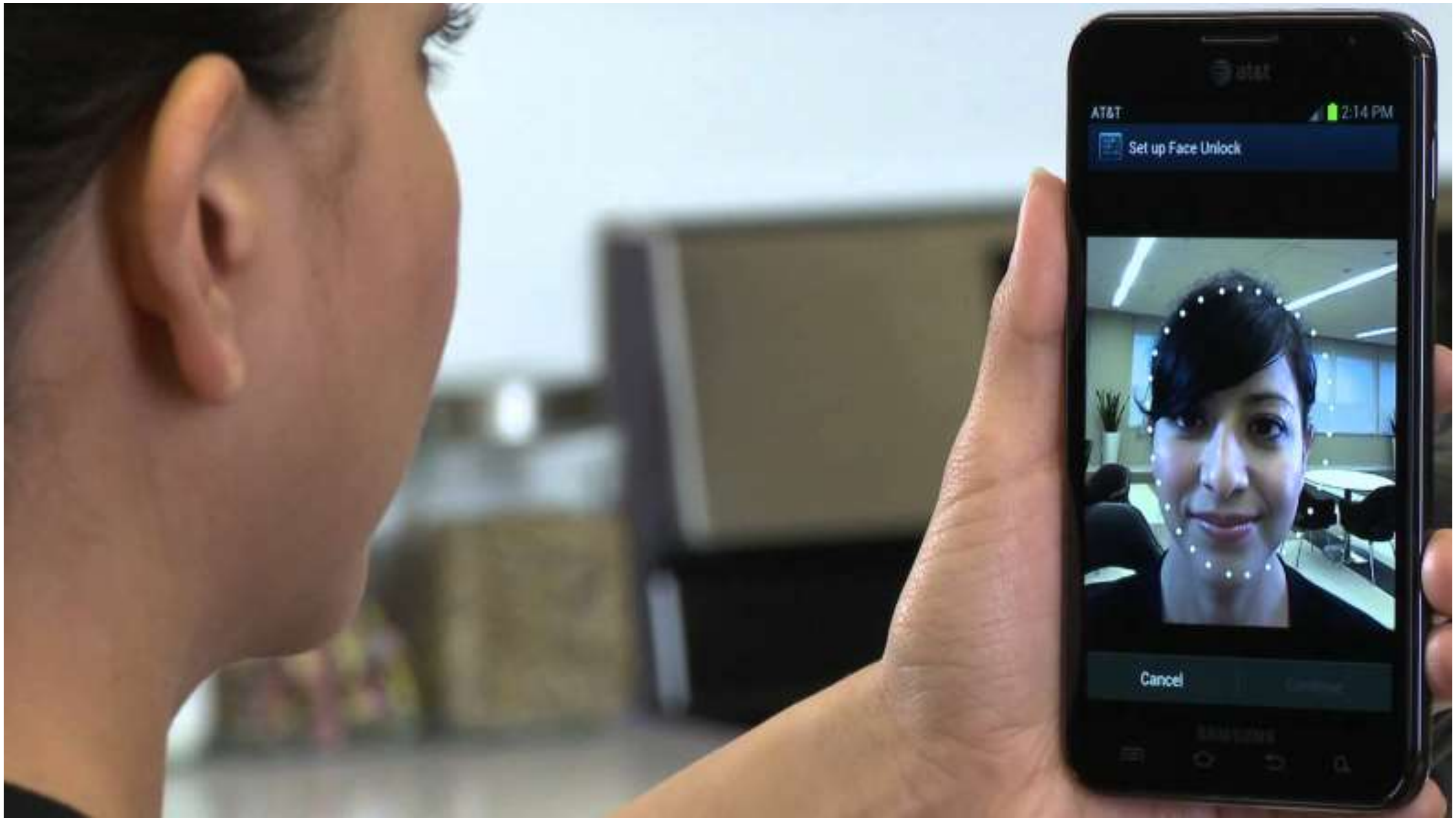
Keep th
bad guys

Don’t lock
me out!

Security
Expert

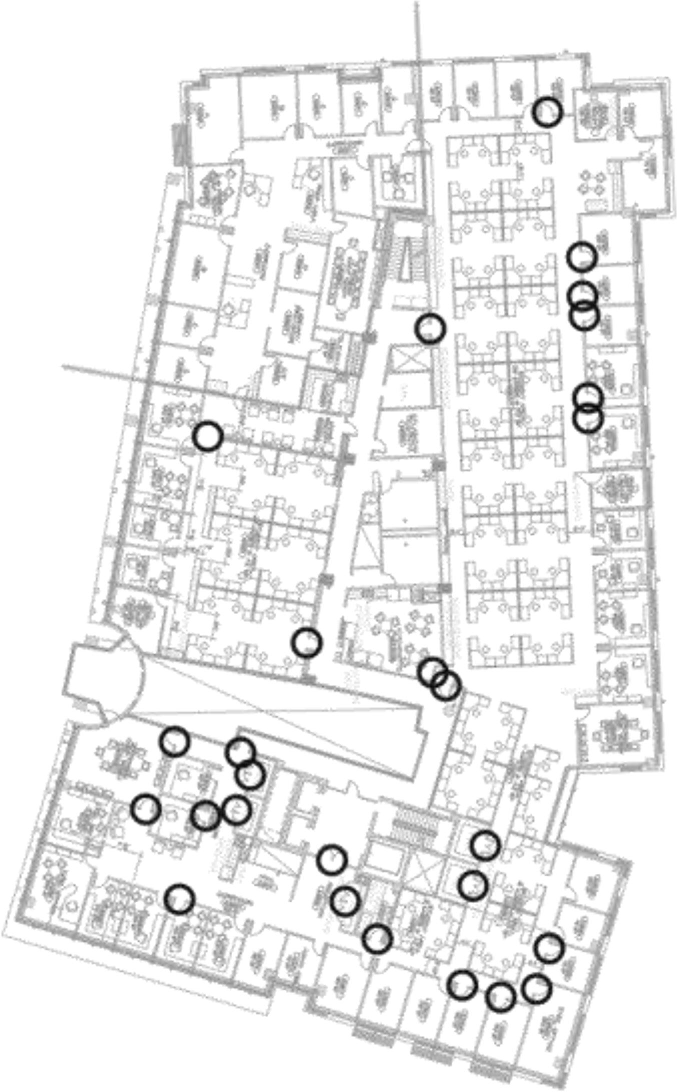
User

Perceptions have an important impact



Perceptions have an important impact

Perceptions have an important impact



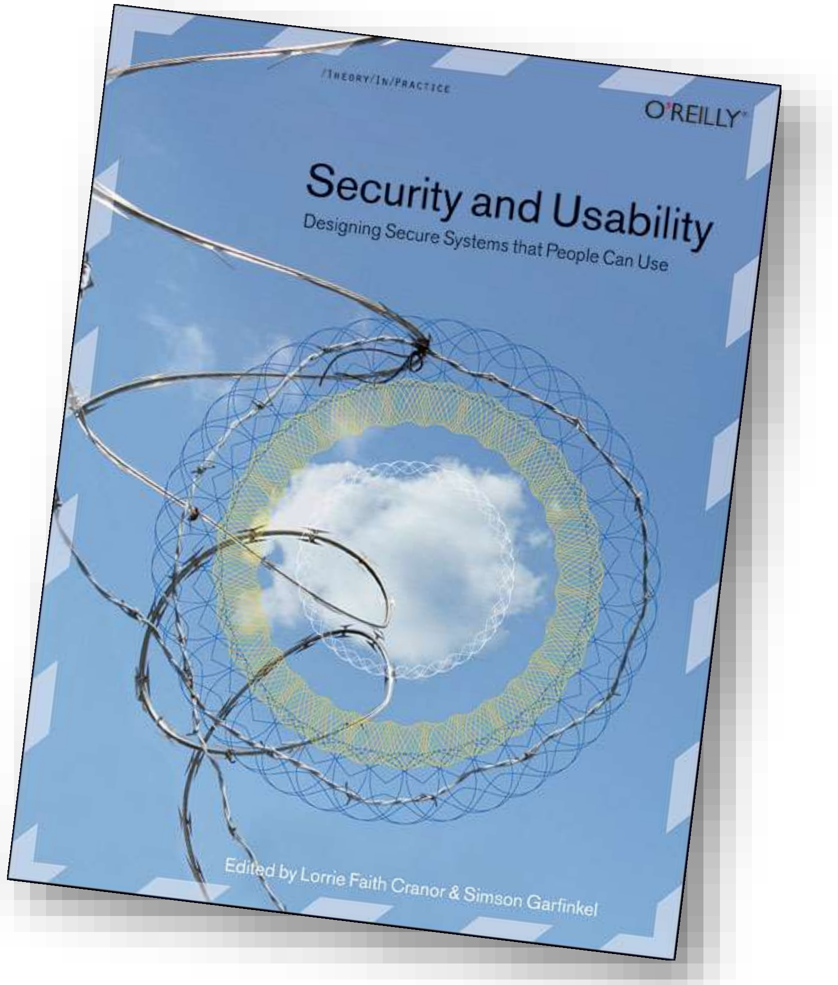
Perceptions have an important impact

“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


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

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

Understand human in the loop

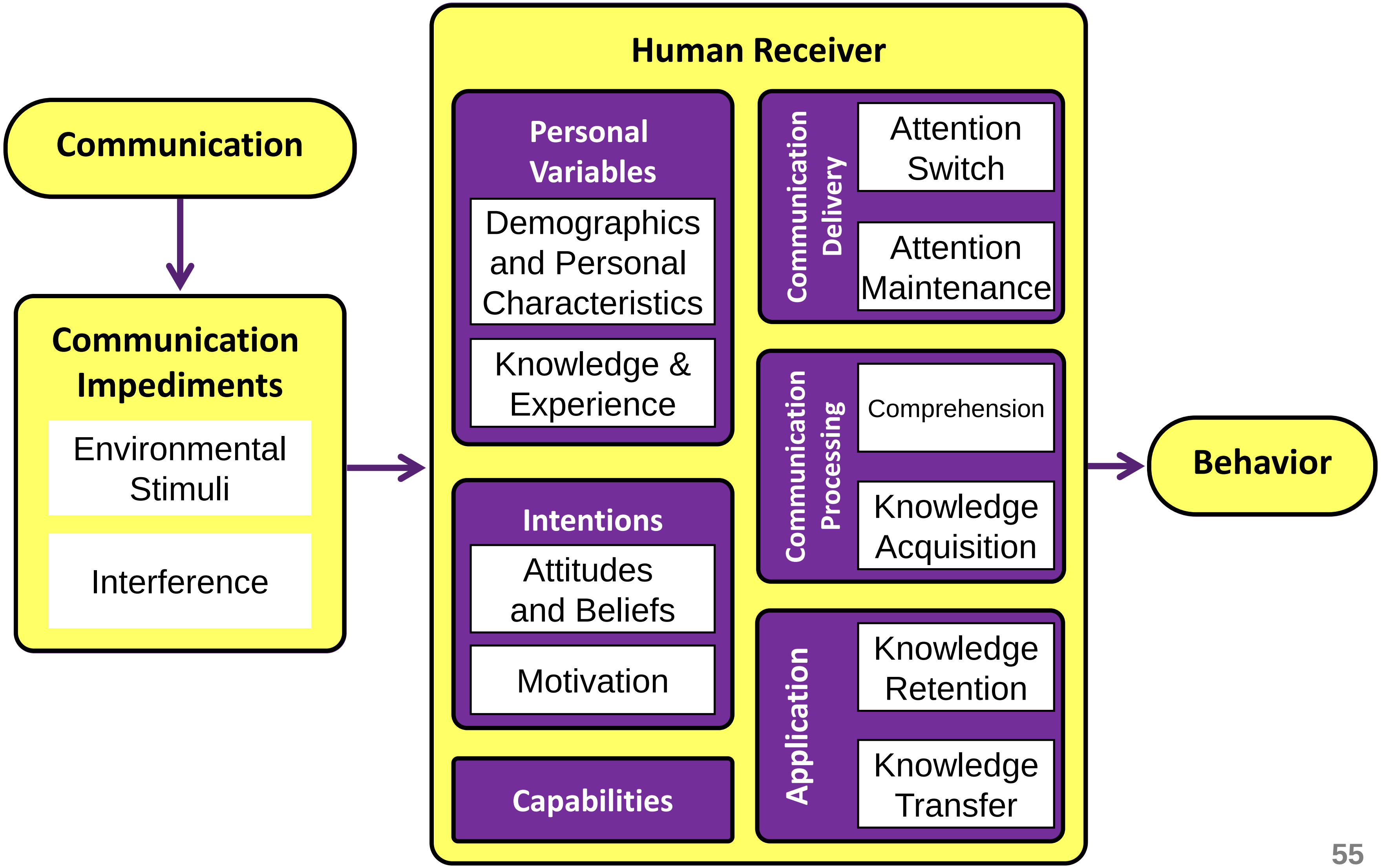
- Do they know they are supposed to be doing something?
- Do they understand what they are supposed to do?
- Do they know how to do it?
- Are they motivated to do it?
- Are they capable of doing it?
- Will they actually do it?

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

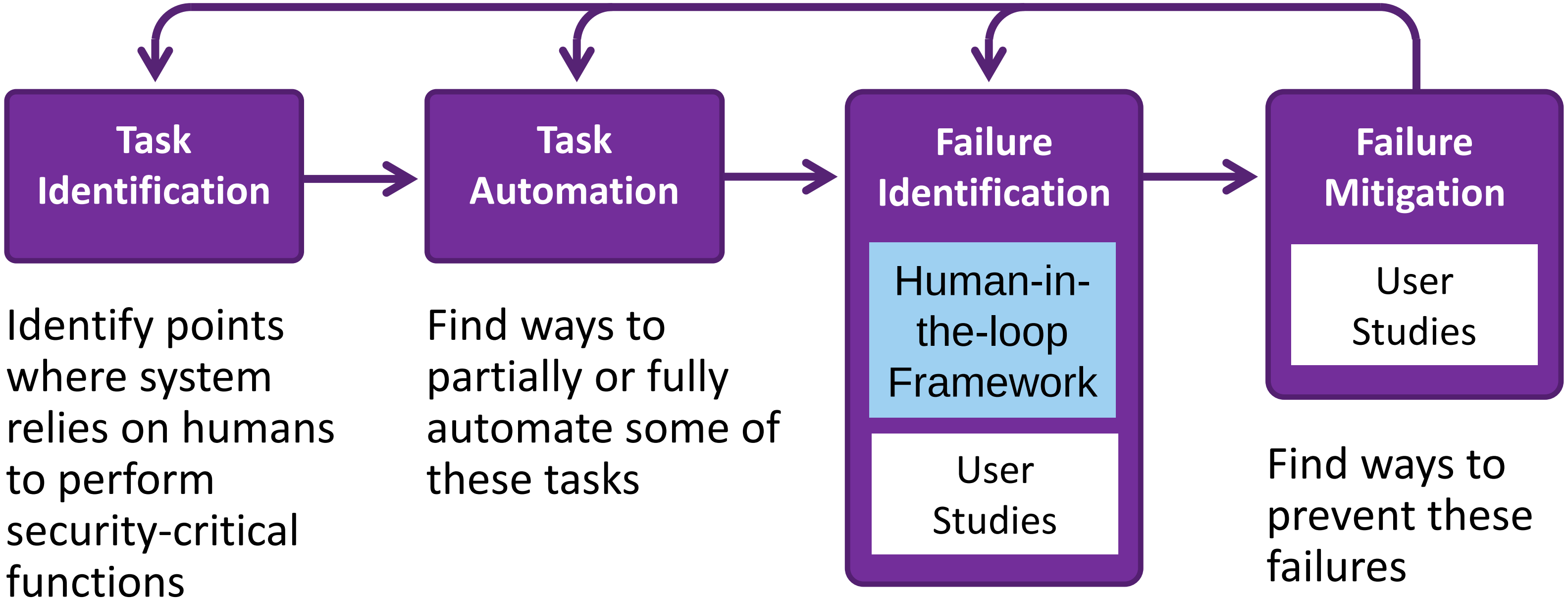
Application

Knowledge Retention

Knowledge Transfer

Behavior

Threat identification & mitigation



Task Identification

Task Automation

Failure Identification

Human-in-the-loop Framework

User Studies

Failure Mitigation

User Studies

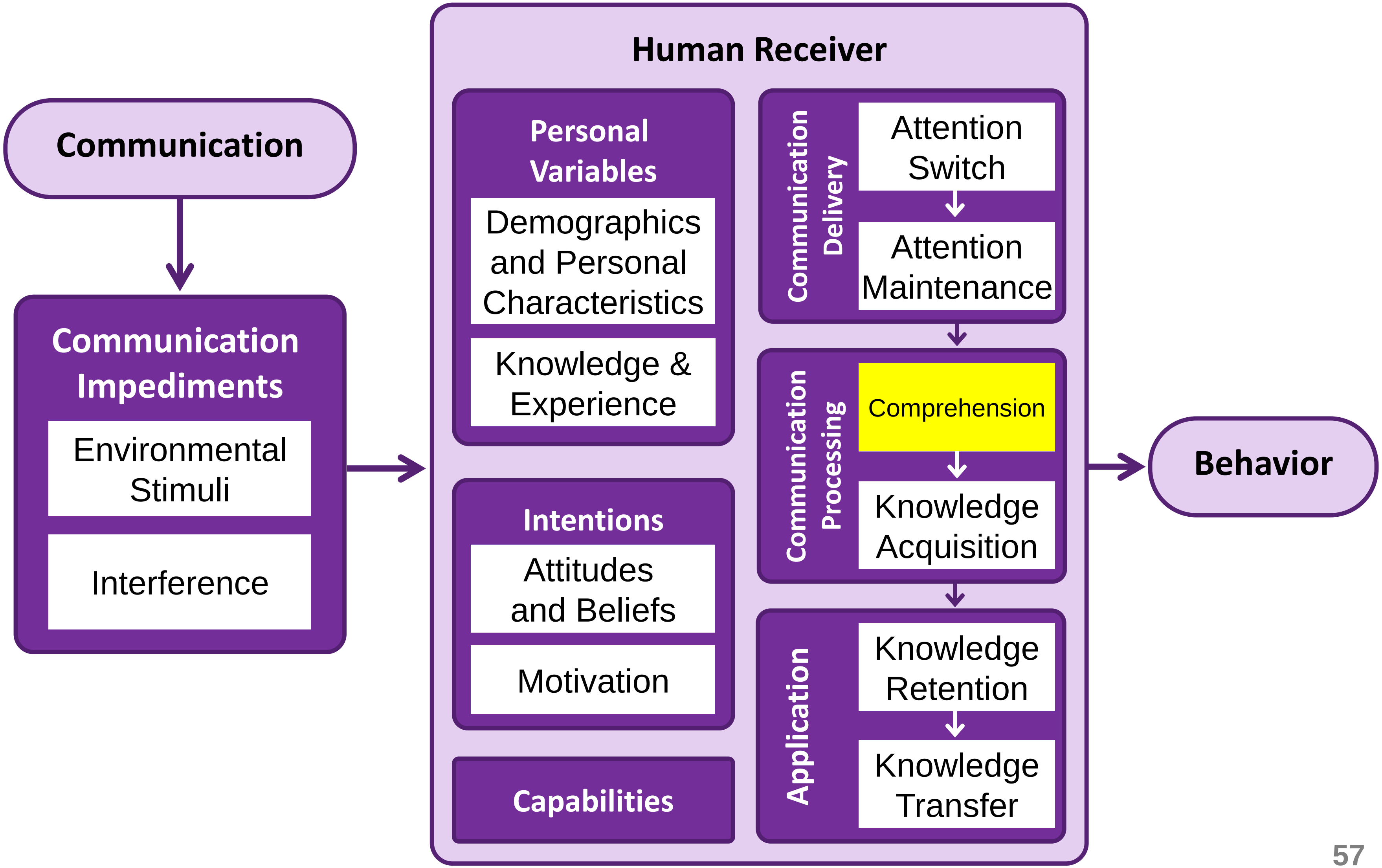
Identify points where system relies on humans to perform security-critical functions

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



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

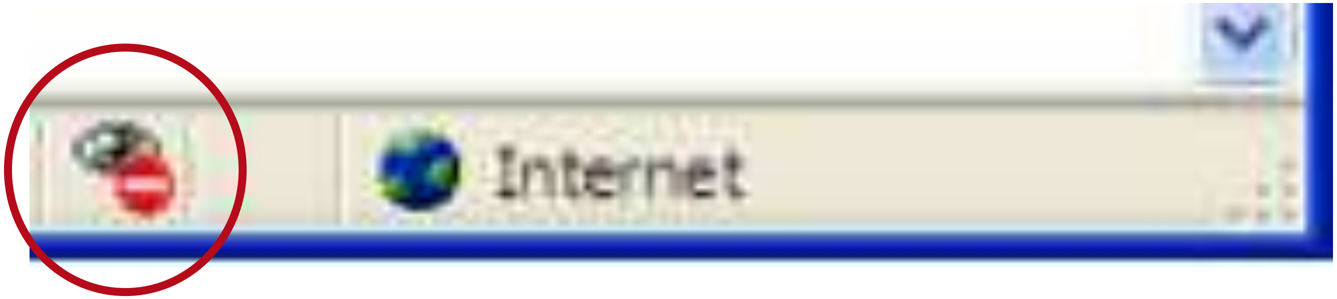
Knowledge Acquisition

Application

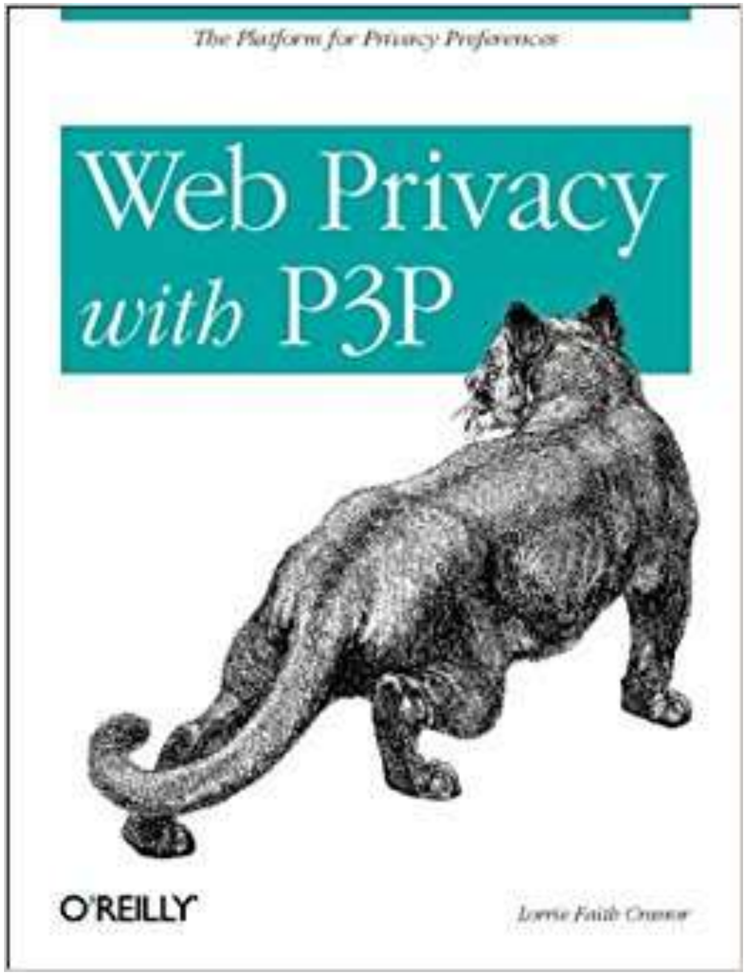
Knowledge Retention

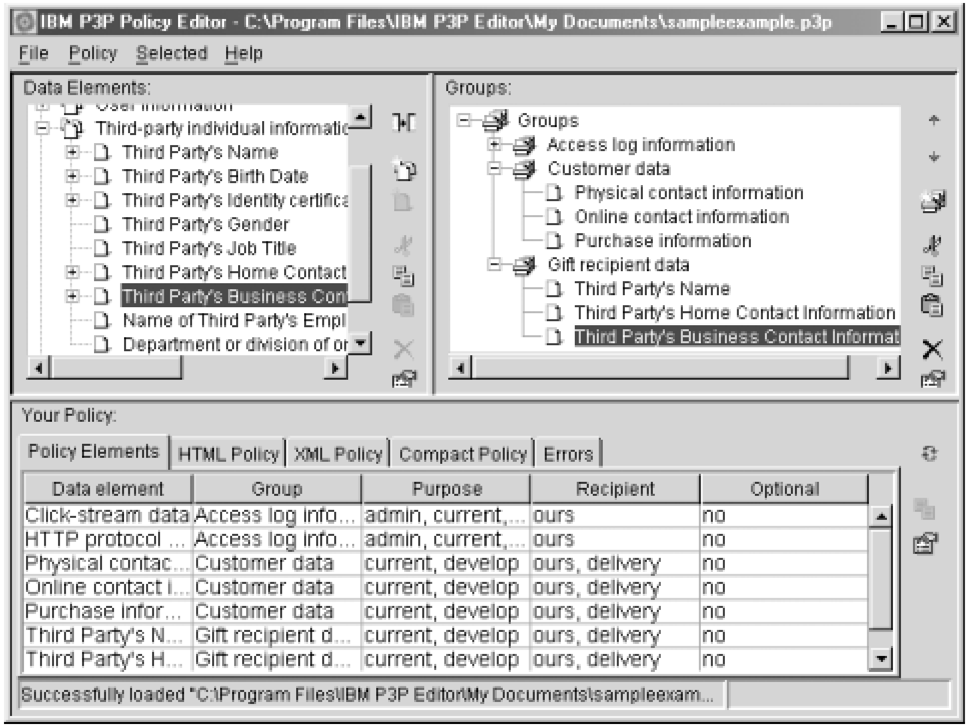
Knowledge Transfer

Behavior



Internet




IBM P3P Policy Editor - C:\Program Files\IBM P3P Editor\My Documents\sampleexample.p3p
File
Policy
Selected
Help
Data Elements:
User Information
Third-party individual informatic
Third Party's Name
Third Party's Birth Date
Third Party's Identity certifica
Third Party's Gender
Third Party's Job Title
Third Party's Home Contact
Third Party's Business Con
Name of Third Party's Empl
Department or division of or
Groups:
Groups
Access log information
Customer data
Physical contact information
Online contact information
Purchase information
Gift recipient data
Third Party's Name
Third Party's Home Contact Information
Third Party's Business Contact Informat
Your Policy:
Policy Elements
HTML Policy
XML Policy
Compact Policy
Errors

Data element	Group	Purpose	Recipient	Optional
Click-stream data	Access log info...	admin, current,...	ours	no
HTTP protocol ...	Access log info...	admin, current,...	ours	no
Physical contac...	Customer data	current, develop	ours, delivery	no
Online contact i...	Customer data	current, develop	ours, delivery	no
Purchase infor...	Customer data	current, develop	ours, delivery	no
Third Party's N...	Gift recipient d...	current, develop	ours, delivery	no
Third Party's H...	Gift recipient d...	current, develop	ours, delivery	no

Successfully loaded "C:\Program Files\IBM P3P Editor\My Documents\sampleexam...