01. Course Overview; Introduction to Usable Security & Privacy

Blase Ur, March 27th, 2017
CMSC 23210 / 33210
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.”

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

<table>
<thead>
<tr>
<th>Security</th>
<th>Usability/HCI</th>
<th>Usable Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the space of possible passwords?</td>
<td>How difficult is it for a user to create, remember, and enter a password? How long does it take?</td>
<td>All the security/privacy and usability HCI questions</td>
</tr>
<tr>
<td>How can we make the password space larger to make the password harder to guess?</td>
<td>How hard is it for users to learn the system?</td>
<td>How do users select passwords? How can we help them choose passwords harder for attackers to predict?</td>
</tr>
<tr>
<td>How are the stored passwords secured?</td>
<td>Are users motivated to put in effort to create good passwords?</td>
<td>As the password space increases, what are the impacts on usability factors and predictability of human selection?</td>
</tr>
<tr>
<td>Can an attacker gain knowledge by observing a user entering her password?</td>
<td>Is the system accessible for users of all abilities?</td>
<td></td>
</tr>
</tbody>
</table>
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
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?
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.
Security warnings (4/12)

• Can we make them more effective?
Can people want to share some things widely yet want other things to be private?
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?
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?
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?
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 the bad guys out

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
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

Human-in-the-loop framework

**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**: 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**: Identify potential failure modes for remaining tasks.

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

- **Human-in-the-loop Framework**
  - User Studies
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
Web Privacy with P3P

![Book Cover](image)

![IBM P3P Policy Editor Screenshot](image)

---

<table>
<thead>
<tr>
<th>Policy Elements</th>
<th>HTML Policy</th>
<th>XML Policy</th>
<th>Compact Policy</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data element</td>
<td>Group</td>
<td>Purpose</td>
<td>Recipient</td>
<td>Optional</td>
</tr>
<tr>
<td>Click-stream data</td>
<td>Access log info</td>
<td>admin, current</td>
<td>ours</td>
<td>no</td>
</tr>
<tr>
<td>HTTP protocol</td>
<td>Access log info</td>
<td>admin, current</td>
<td>ours</td>
<td>no</td>
</tr>
<tr>
<td>Physical contact</td>
<td>Customer data</td>
<td>current, develop</td>
<td>ours, delivery</td>
<td>no</td>
</tr>
<tr>
<td>Online contact</td>
<td>Customer data</td>
<td>current, develop</td>
<td>ours, delivery</td>
<td>no</td>
</tr>
<tr>
<td>Purchase info</td>
<td>Customer data</td>
<td>current, develop</td>
<td>ours, delivery</td>
<td>no</td>
</tr>
<tr>
<td>Third Party's N</td>
<td>Gift recipient data</td>
<td>current, develop</td>
<td>ours, delivery</td>
<td>no</td>
</tr>
<tr>
<td>Third Party's H</td>
<td>Gift recipient data</td>
<td>current, develop</td>
<td>ours, delivery</td>
<td>no</td>
</tr>
</tbody>
</table>

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