01 Course overview and introductions

Lujo Bauer, Nicolas Christin, and Abby Marsh

January 11, 2016

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security
Today’s class

• Course staff introductions
• Usable security and privacy = ???
• Overview of course topics
• Course policies / syllabus
• Student introductions
Who we are

• Lujo Bauer   lbauer@cmu.edu

• Associate Professor of Electrical and Computer Engineering & Computer Science

• Interests: computer security, usable security, passwords, information-flow-control, …

• Office hours: by appointment
Who we are

• Nicolas Christin nicolasc@cmu.edu

• Assistant Research Professor of Electrical and Computer Engineering & Engineering and Public Policy

• Interests: computer security, usable security, passwords, online crime, security and policy…

• Office hours: by appointment
Who we are

• Abigail Marsh  acmarsh@cmu.edu
• PhD Student in the Institute for Software Research
• Interests: digital privacy, usable privacy, adolescent technology users, other minority user experiences, ...
• Office hours: by appointment
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.”

Better together

Examining security/privacy and usability together is often critical for achieving either
Interdisciplinary approach useful

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

- Psychology
- Sociology
- Ethnography
- Cognitive sciences
- Warnings science
- Risk perception
- Organizational change
- Behavioral economics
- HCI
- Marketing
- Counterterrorism
- 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
Usable security research bridges security and usability

<table>
<thead>
<tr>
<th>Security</th>
<th>Usability/HCI</th>
<th>Usable Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humans are a secondary constraint to security constraints</td>
<td>Humans are the primary constraint, security rarely considered</td>
<td>Human factors and security are both primary constraints</td>
</tr>
</tbody>
</table>
Usable security research bridges security and usability

<table>
<thead>
<tr>
<th>Security</th>
<th>Usability/HCI</th>
<th>Usable Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Humans are a secondary constraint to security constraints</td>
<td>Humans are the primary constraint, security rarely considered</td>
<td>Human factors and security are both primary constraints</td>
</tr>
<tr>
<td>Humans considered primarily in their role as adversaries/attackers</td>
<td>Concerned about human error but not human attackers</td>
<td>Concerned about both normal users and adversaries</td>
</tr>
<tr>
<td>Involves threat models</td>
<td>Involves task models, mental models, cognitive models</td>
<td>Involves threat models AND task models, mental models, etc.</td>
</tr>
<tr>
<td>Focus on security metrics</td>
<td>Focus on usability metrics</td>
<td>Considers usability and security metrics together</td>
</tr>
<tr>
<td>User studies rarely done</td>
<td>User studies common</td>
<td>User studies common, often involve deception + active adversary</td>
</tr>
</tbody>
</table>
User-selected graphical 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 graphical 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 using a variety of devices, for users with disabilities? All the security/privacy and usability HCI questions. How do users select graphical 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?
# User-selected graphical 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 <em>difficult</em> is it for a <em>user</em> to create, remember, and enter a graphical 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 <em>users</em> select graphical passwords? How can we help them choose passwords harder for <em>attackers</em> to predict?</td>
</tr>
<tr>
<td>How are the stored passwords secured?</td>
<td>Are users <em>motivated</em> 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 <em>attacker</em> gain knowledge by observing a user entering her password?</td>
<td>Is the system <em>accessible</em> using a variety of devices, for users with disabilities?</td>
<td></td>
</tr>
</tbody>
</table>
Goals for this course

• Gain an appreciation for the importance of usability within security and privacy
  – HCI → Security & Privacy, and vice versa

• Learn about current research in usable privacy and security

• Learn how to conduct usability studies

• Learn how to critically examine UPS studies you hear about or read about
Policies and logistics

• Updated syllabus is always available: https://cups.cs.cmu.edu/courses/ups-sp16/
Which course #?

• Ph.D. students must take 05-836 (HCII) or 08-734 (ISR) or 19-734 (EPP) for 12 units
• Undergrads: 05-436 or 08-534 or 19-534 for 9 units
• Master’s students: check with your program
• If you switch sections, you will be waitlisted (but we will let you in)
Components of your grade

- Homework: 20%
- Quizzes: 20%
- Midterms: 20%
- Class Project: 40%
Readings

• Generally one required reading per class
  – There will be quizzes – see next slide
• Complete the readings before class
• Textbook: Lazar et al.’s *Research Methods in Human-Computer Interaction*
• Most readings from recent conferences
• 12-unit students: one additional reading for most classes (see homeworks)
Quizzes

• Given in the first five minutes of class
  – End at 3:05pm

• Will be a quick quiz based on that day’s required reading

• Three lowest quiz scores dropped

• If you will be unable to arrive on time for a class, submit a reading summary and highlight of the required readings before class by email
  – Must have reason why can’t arrive on time
Homework

• 10 homework assignments
  – Drop single lowest grade
  – 4 total grace days (day = 24h) for semester
    • Max 2 for any single homework
    • Beyond grace days, no late homework accepted!
    • Late homeworks must be submitted via mailing list

• For 12-unit Students
  – These will include a “reading summary” of one optional reading per class
  – 3 to 7 sentence summary
  – One “highlight”
What is the homework 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
- Other activities

*Homework 1 is already posted (and due Jan 25)!*
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 (two of them)

• Given about one-third and two-thirds of the way through the class
• 20% of your grade
• 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 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, IRB application, progress report & presentation, final paper, and a final presentation

• Submit a poster to SOUPS 2016 and a paper to another conference
Projects from prior UPS courses

• The Post that Wasn't: Exploring Self-Censorship on Facebook (CSCW ‘13)

• How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation (USENIX Security ‘12)

• 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)

• To Update or Not to Update: Review-Based Notifications for Android App Updates

• Passwords Gone Mobile: An Analysis of the Usability and Security of Text Passwords on Mobile Devices
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
Academic integrity

• Make yourself familiar with CMU’s policies about plagiarism and academic integrity

• Don’t even look at other students’ homework assignments
  – Exception: When we explicitly say that you may work in groups for a particular task

• Quote text and cite ideas that are not yours

• Consequences of cheating and plagiarism range from a 0 on the assignment to expulsion from CMU
Logistics

• There is no final exam
  – Project presentations during final exam period

• We have no Blackboard site

• Please use Piazza for questions:
  https://piazza.com/class/ij5wty5ksobtt

• Use the instructor mailing list to contact us or submit homework:
  ups-class-instructors@lists.andrew.cmu.edu

• You may wish to join the CUPS mailing list
  – Weekly CUPS lunch (Thursdays @ Noon)
  – News and opportunities of interest
  – To sign up, follow link on course webpage
Course topics

• 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
  – Overview of statistics

• Quick overviews of security and privacy

• Specific usable privacy and security topics
Topic: 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.
Topic: Secondary authentication

- Mother’s maiden name?
- Favorite athlete?
- A code sent to your phone?
Topic: Privacy Tools

• How can tools help users protect their privacy?

• How usable are those tools?
Topic: UPS in the home

- The home is becoming a tangled mess of devices, files, and sensors... what do we do about it?
Topic: Software Updates and Mobile App Updates

• Software is constantly changing.
• Are users able to make correct decisions about whether to accept new updates?
• Should they need to?
Topic: Security warnings

- Can we make them more effective?
Topic: Smartphones and UPS

• Do people understand where the information on their phone goes?

• …And can someone please make app permissions usable?
Topic: Mobile and UbiComp

• What are the privacy and security implications of devices that go wherever you go?

• How can that be addressed?
Topic: Privacy policies and notices

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

Amazon Privacy Policy

<table>
<thead>
<tr>
<th>Types of Information</th>
<th>how we use your information</th>
<th>who we share your information with</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>provide services &amp; maintain site</td>
<td>research &amp; development</td>
</tr>
<tr>
<td>contact information</td>
<td>opt in</td>
<td>opt out</td>
</tr>
<tr>
<td>cookies</td>
<td>opt in</td>
<td>opt out</td>
</tr>
<tr>
<td>demographic information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>financial information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>health information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>preferences</td>
<td></td>
<td></td>
</tr>
<tr>
<td>purchasing information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>social security number &amp; info ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>your activity on this site</td>
<td></td>
<td></td>
</tr>
<tr>
<td>your exact location</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Screenshot from http://www.tosdr.org

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 business. In the section below, we list the reasons financial companies can share their
Topic: Biometrics

• Characteristics of the human body can be used to identify or authenticate
  – How can this be done in a user-friendly way?
Topic: Usable encryption

• Why don’t people encrypt their email and their files?
Topic: Browser privacy & security

• What kinds of tracking currently occurs, and what do average people think of it?

• ... And why has phishing been so effective?
Topic: SSL and PKIs

- Is there any hope for making certificates and SSL warnings usable?
Topic: Social networks and privacy

- 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.
- Select Apps you 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 these 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 settings.
- 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 settings.
Topic: Trust and mental models

• How do average people think about privacy and security, and how can we help them and educate them?

Image from http://www.quickmeme.com
Topic: UPS in safety-critical devices

• Some cars, medical devices, and household appliances contain computers
  – How do we help users protect their privacy and maintain security while still reaping the benefits of these new technologies?
Topic: Usable access control

- Controlling who has access to your files, physical spaces, and online posts is hard.
Topic: User Education and Behavioral Economics

• How can we encourage (nudge) people to think about privacy and security?
Topic: Non-US Perspectives on Privacy and Research

• How do the topics of this class change as we look at non-US perspectives?

• Is one’s perspective on privacy a function of one’s culture?
Who you are?

• Your preferred name
• Program at CMU (e.g., Privacy Engineering, COS, ECE, Master’s in HCI)
• Why did you sign up for this course?
• Your first (ungraded) quiz