01- Course overview and introductions

Lorrie Cranor and Blase Ur

January 14, 2014

05-436 / 05-836 / 08-534 / 08-734
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

• Lorrie Cranor lorrie@cs.cmu.edu

• Associate Professor of Computer Science and Engineering & Public Policy

• Director, CyLab Usable Privacy and Security Laboratory; used to work for AT&T Labs

• Office hours: Wednesdays 3:00p–4:00p in CIC 2207 or by appointment
Who we are

• Blase Ur  blase@blaseur.com

• Third-year Ph.D. student advised by Lorrie

• Authored 20+ peer-reviewed publications in security, privacy, and usability

• Interests: passwords, OBA, teen-parent privacy, network security, and smart homes

• Office hours: Tuesdays 4:30p–5:30p in CIC 2222 cubicles or by appointment
“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 in which security is not reduced 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</td>
<td>Humans are the primary constraint, security rarely considered</td>
<td>Human factors and security are both primary constraints</td>
</tr>
<tr>
<td>constraints</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Involves threat models
- Involves task models, mental models, cognitive models
- Focus on security metrics
- Focus on usability metrics
- Considers usability and security metrics together
- User studies rarely done
- User studies common, often involve deception + active adversary
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

<table>
<thead>
<tr>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is the space of possible passwords?</td>
</tr>
<tr>
<td>How can we make the password space larger to make the password harder to guess?</td>
</tr>
<tr>
<td>How are the stored passwords secured?</td>
</tr>
<tr>
<td>Can an <strong>attacker</strong> gain knowledge by observing a user entering her password?</td>
</tr>
</tbody>
</table>
# 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 difficult is it for a <strong>user</strong> 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 <strong>users</strong> select graphical passwords? How can we help them choose passwords harder for <strong>attackers</strong> to predict?</td>
</tr>
<tr>
<td>How are the stored passwords secured?</td>
<td>Are users <strong>motivated</strong> 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 <strong>attacker</strong> gain knowledge by observing a user entering her password?</td>
<td>Is the system <strong>accessible</strong> 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 security and privacy
• Learn how to conduct usability studies
• Gain tools for critically examining studies you hear about or read about
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
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.

Image from http://www.trypap.com
Topic: Secondary authentication

- Mother’s maiden name?
- Favorite athlete?
- Make of first car?
- Where Sarah Palin met her husband?
Topic: Censorship, anonymity

• How can we help people who wish to remain anonymous on the Internet do so?

• How can we help people who wish to evade censorship do so? (And should we?)

The problem with censorship is
Topic: UPS in the home

- The home is becoming a tangled mess of devices, files, and sensors... what do we do about it?
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: 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>context information</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>cookies</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>demographic information</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>financial information</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>health information</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>preferences</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>purchasing information</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>social security number &amp; grant ID</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>your activity on this site</td>
<td>opt out</td>
<td>opt in</td>
</tr>
<tr>
<td>your exact location</td>
<td>opt out</td>
<td>opt in</td>
</tr>
</tbody>
</table>

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 businesses. In the section below, we list the reasons financial companies can share their information.
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?
Topic: Trust and mental models

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

Image from http://www.motortrend.com
Image from http://www.hcwreview.com
Image from http://www.allaboutsymbian.com
Topic: Usable access control

• Controlling who has access to your files, physical spaces, and online posts is hard
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: Economics and behavior

• How can we encourage (nudge) people to think about privacy and security?

• …And why do Nigerian scammers say they are from Nigeria?

Don't come crying to me when you're hacked.
Topic: Graphical passwords

- Humans have great visual memory… can this fact be leveraged for authentication?

Image from http://www.techradar.com
Policies and logistics

• Updated syllabus is always available: http://cups.cs.cmu.edu/courses/ups-sp14/

• Right now: Swap lecture 2 and 3 on the printed version
Which course #?

- Ph.D. students must take 05-836 (HCII) or 08-734 (ISR) for 12 units
- Undergrads: 05-436 or 08-534 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: 35% (12-unit) or 50% (9-unit)
- Research project: 40%
- Class presentation: 15% (12-unit only)
- Class participation: 10%
Readings

• Generally two required readings per class
  – More in the first few weeks
• Textbook: Lazar et al.’s *Research Methods in Human-Computer Interaction*
• Most readings from recent conferences
• Complete the readings *before* class
• 12-unit students: one optional reading for each homework
Homework

• 11 homework assignments
  – Drop single lowest grade
  – No late homework accepted!

• Part 1: Reading summaries
  – All required and (for 12-unit students) one optional reading
  – 3 to 7 sentence summary
  – One “highlight”
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.
Homework

• Parts 2+: Activities
  – Conduct mini studies and report results (Up to $15 out of pocket to run on Mechanical Turk)
  – Evaluate the incidence or state of something in the real world
  – Conduct usability evaluations of tools
  – Propose possible studies
  – Other activities
Project

• Design, conduct, and analyze a user study in usable privacy or security
  – Groups assigned based on your preferences

• Deliverables: Project proposal, IRB application, progress report & presentation, final paper, and a final presentation

• Submit a poster to SOUPS 2014 and a paper to another conference
Projects from the last UPS course

- 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)
- What Do Online Behavioral Advertising Disclosures Communicate to Users? (WPES ‘12)
- QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks (USEC ‘13)
- The Usability of Computer Forensics Tools
- The Usability of Icons for Privacy
Class presentation

• 12-unit students only!
• Lead class for 30 minutes on assigned day
• Do all required & optional readings
• Don’t just present reading summaries!
• Do conduct demos or activities, lead discussions, design user studies, etc.
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

• 10% of your grade
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 range from a 0 on the assignment to expulsion from CMU
Logistics

• There are no exams
  – Project presentations during final exam period
• We have no Blackboard site
• We will sign you up for a course e-mail list
• You may wish to join the CUPS mailing list
  – Weekly CUPS lunch (Wednesdays @ Noon)
  – News and opportunities of interest
  – To sign up, follow link on course webpage
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?