Security and human behavior

Some material from Lorrie Cranor, Mike Reiter, Rob Reeder, Blase Ur
In these lectures …

• Overview
• Minimizing effort
• Case studies
  – Grey, password expiration, security images, password meters, implantable devices
• Making things better
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.”

More on humans

“Not long ago, [I] received an e-mail purporting to be from [my] bank. It looked perfectly legitimate, and asked [me] to verify some information. [I] started to follow the instructions, but then realized this might not be such a good idea … [I] definitely should have known better.”

-- former FBI Director Robert Mueller
And one more …

“I think privacy is actually overvalued … If someone drained my cell phone, they would find a picture of my cat, some phone numbers, some email addresses, some email text. What’s the big deal?”

-- Judge Richard Posner
U.S. Court of Appeals, 7th circuit
Better together

Examining security/privacy and usability together is often critical for achieving either
The human threat

- Malicious humans
- Humans who don’t know what to do
- Unmotivated humans
- Humans with human limitations
Key challenges

• Security is a **secondary task**
  – Users are trying to get something else done

• Security concepts are **hard**
  – Viruses, certificates, SSL, encryption, phishing

• Human capabilities are **limited**
Are you capable of remembering a unique strong password for every account you have?
Key challenges

• Security is a secondary task
• Security concepts are hard
• Human capabilities are limited
• Misaligned priorities
Keep the bad guys out!

Don’t lock me out!

Security Expert

User
Key challenges

• Security is a **secondary task**
• Security concepts are **hard**
• Human capabilities are **limited**
• Misaligned **priorities**
• **Active adversaries**
  – Unlike ordinary UX
What is Twitter?

Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick, frequent answers to one simple question: What are you doing?
Key challenges

• Security is a secondary task
• Security concepts are hard
• Human capabilities are limited
• Misaligned priorities
• Active adversaries
  – Unlike ordinary UX
• Habituation
  – The “crying wolf” problem
KEY CHALLENGE EXAMPLE:

HABITUATION
Exercise: Draw a penny

• Draw a circle

• Sketch the layout of the four basic items on the front of a US penny
  – What are the items, and how are they positioned?

• Hint:
  – Someone’s portrait (who?)
  – Two patriotic phrases
  – Another item
  – Extra credit: an item that some pennies have and some don’t
Score your sketch

• Score:
  – 1 for Abraham Lincoln
  – +1 for Abraham Lincoln facing right
  – +1 for “Liberty”
  – +1 for “Liberty” to Abe’s left
  – +1 for “In God We Trust”
  – +1 for “In God We Trust” over Abe’s head
  – +1 for the year
  – +1 for the year to Abe’s right
  – Extra credit: +1 for the mint letter under the year
  – -1 for every other item
Lessons from Abe

• You’ve probably seen hundreds of pennies
  – And yet, this is hard

• Memory limitations
  – Remembering a penny isn’t important, unless you take this quiz!

• Habituation
  – You see it so often, you don’t remember it anymore
Habituation to warnings
Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegafonc.
If it’s important, make it stand out

**SSL warning; risk low; yellow background**

**Malware warning; risk very high; red background**
MINIMIZING EFFORT
People are economical

• Given two paths to a goal, they’ll take the shorter path

• More steps = less likely they’ll be completed

• Can they figure out what to do?
  – Too hard = give up and take easiest path
You should only open attachments from a trustworthy source.

Attachment: TUX Scope Framing and Ownership
091211b.pptx from Inbox - Microsoft Outlook

Would you like to open the file or save it to your computer?

Open  Save  Cancel

Always ask before opening this type of file
You should only open attachments from a trustworthy source.

Attachment: TUX Scope Framing and Ownership
091211b.pptx from Inbox - Microsoft Outlook

Would you like to open the file or save it to your computer?

Open  Save  Cancel

Always ask before opening this type of file
What’s the source of this attachment?
What’s the source of this attachment?

What makes a source trustworthy or not trustworthy?
What’s the source of this attachment?

What makes a source trustworthy or not trustworthy?

What will happen if I don’t follow this advice?
What’s the source of this attachment?

What makes a source trustworthy or not trustworthy?

What will happen if I don’t follow this advice?

Does this mean that opening is dangerous but saving is safe?
What’s the source of this attachment?

What makes a source trustworthy or not trustworthy?

What will happen if I don’t follow this advice?

What steps can I take to decide what to do?

Does this mean that opening is dangerous but saving is safe?
Good security practices that people don’t do

• Install anti-virus software
• Keep your OS and applications up-to-date
• Change your passwords frequently *
• Read a website’s privacy policy before using it
• Regularly check accounts for unusual activity
• Pay attention to the URL of a website
• Research software’s reputation before installing
• Enable your software firewall
• Make regular backups of your data
• Read EULAs before installing software
What can go wrong when you don’t consider human factors

CASE STUDIES
GREY AND USER BUY-IN
Is Grey too slow?

• Grey: Smartphone-based access control
  – (Covered earlier in the semester)
  – Strong security benefits vs. keys

• Users complained about speed
  – Videotaped a door to measure vs. keys

[Bauer et. al, SOUPS 2007]
Average access times

Grey is not noticeably slower than keys!

Getting keys
3.6 sec
σ = 3.1
Stop in front of door
5.4 sec
σ = 3.1
Door opened
5.7 sec
σ = 3.6
Door Closed
Total
14.7 sec
σ = 5.6

Getting phone
8.4 sec
σ = 2.8
Stop in front of door
2.9 sec
σ = 1.5
Door opened
3.8 sec
σ = 1.1
Door Closed
Total
15.1 sec
σ = 3.9

σ
Grey is not noticeably slower than keys!
“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.”

Takeaway: Misaligned priorities
PASSWORD EXPIRATION AND USER BEHAVIOR
Does password expiration improve security in practice?

• **Observation**
  – Users often respond to password expiration by transforming their previous passwords in small ways [Adams & Sasse 99]

• **Conjecture**
  – Attackers can exploit the similarity of passwords in the same account to predict the future password based on the old ones [Zhang et. al, CCS 2010]
Empirical analysis

• UNC “Onyen” logins
  – Broadly used by campus and hospital personnel
  – Password change required every 3 months
  – No repetition within 1 year

• 51141 unsalted hashes, 10374 defunct accounts
  – 4 to 15 hashes per account in temporal order

• Cracked ~8k accounts, 8 months, standard tools

• Experimental set: 7752 accounts
  – At least one cracked password, NOT the last one
Transform Trees

- Approximation algorithm for optimal tree searching
## Location Independent Transforms

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capitalization</td>
<td>tarheels#1 → tArheels#1</td>
</tr>
<tr>
<td>Deletion</td>
<td>tarheels#1 → tarheels1</td>
</tr>
<tr>
<td>Duplication</td>
<td>tarheels#1 → tarheels#11</td>
</tr>
<tr>
<td>Substitution</td>
<td>tarheels#1 → tarheels#2</td>
</tr>
<tr>
<td>Insertion</td>
<td>tarheels#1 → tarheels#12</td>
</tr>
<tr>
<td>Leet Transform</td>
<td>tarheels#1 → t@c@rheels#1</td>
</tr>
<tr>
<td>Block Move</td>
<td>tarheels#1 → #tarheels1</td>
</tr>
<tr>
<td>Keyboard Transform</td>
<td>tarheels#1 → tarheels#!</td>
</tr>
</tbody>
</table>
Evaluation

• Pick a known plaintext, non-last password (OLD)
• Pick any later password (NEW)
• Attempt to crack NEW with transform tree rooted at OLD
Results: Offline Attack

Takeaway: Memory limitations, convenience
SECURITY IMAGES AND THE ADVERSARY PROBLEM
If you do not recognize your Personal Security Image & Caption then DO NOT enter your password!
Study design

• Participants recruited via MTurk

• Each day, receive an email with a small $ amount. Log in and “report” the deposit.

• At the end of the study, receive the amount “deposited.”

• On last day, security image is absent: “Under maintenance.”

• Will participants log in?
Varieties of security images

• Control
• Large, blinking
• Interactive (click, type a word)
• Custom image
• No caption
• Also: security priming, less habituation
Results

• 80-100% claimed they looked at the image, but:
  • 73% entered passwords despite no image
  • No significant differences by image type
  • Users with stronger passwords logged in less often (65% to 80%)

Takeaway: Attention failure, misaligned priorities, misunderstanding security concepts
PASSWORD METERS AND MOTIVATING YOUR USERS
Password Meters ... 
• ... come in all shapes and sizes

[Ur et. al, USENIX Sec 2012]
Experimental setup

• No meter
• Baseline (boring) meter
• Visual differences
  – Size, text only
• Dancing bunnies (wait and see)
• Scoring differences
  – Same password scores differently
# Conditions with Visual Differences

<table>
<thead>
<tr>
<th>Condition</th>
<th>Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type new password:</td>
<td>8-character minimum; case sensitive</td>
</tr>
<tr>
<td>Baseline meter</td>
<td>Bad. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>Three-segment</td>
<td>Bad. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>Green</td>
<td>Bad. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>Tiny</td>
<td>Bad. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>Huge</td>
<td>Bad. Consider adding a digit or making your password longer.</td>
</tr>
<tr>
<td>No suggestions</td>
<td>Bad.</td>
</tr>
<tr>
<td>Text-only</td>
<td>Bad. Consider adding a digit or making your password longer.</td>
</tr>
</tbody>
</table>
Conditions with Visual Differences

Type new password: [user]

8-character minimum; case sensitive

Baseline meter
Bad. Consider adding a digit or making your password longer.

Three-segment
Bad. Consider adding a digit or making your password longer.

Green
Bad. Consider adding a digit or making your password longer.

Tiny
Bad. Consider adding a digit or making your password longer.

Huge
Bad. Consider adding a digit or making your password longer.

No suggestions
Bad.

Text-only
Bad. Consider adding a digit or making your password longer.
Conditions with Visual Differences

Type new password: [userlnX]
8-character minimum; case sensitive

Baseline meter
Fair. Consider adding a digit or making your password longer.

Three-segment
Fair. Consider adding a digit or making your password longer.

Green
Fair. Consider adding a digit or making your password longer.

Tiny
Fair. Consider adding a digit or making your password longer.

Huge
Fair. Consider adding a digit or making your password longer.

No suggestions
Fair.

Text-only
Fair. Consider adding a digit or making your password longer.
Conditions with Visual Differences

Type new password: usenlX$1
8-character minimum; case sensitive

Baseline meter: Good. Consider adding a digit or making your password longer.

Three-segment: Good. Consider adding a digit or making your password longer.

Green: Good. Consider adding a digit or making your password longer.

Tiny: Good. Consider adding a digit or making your password longer.

Huge: Good. Consider adding a digit or making your password longer.

No suggestions: Good.

Text-only: Good. Consider adding a digit or making your password longer.
Conditions with Visual Differences

Type new password: usenIX$$e5
8-character minimum; case sensitive

Baseline meter: Excellent!

Three-segment: Excellent!

Green: Excellent!

Tiny: Excellent!

Huge: Excellent!

No suggestions: Excellent!

Text-only: Excellent!
# Conditions with Visual Differences

<table>
<thead>
<tr>
<th>Type new password:</th>
<th>user!X$e5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Baseline meter</strong></td>
<td>Excellent!</td>
</tr>
<tr>
<td><strong>Three-segment</strong></td>
<td>Excellent!</td>
</tr>
<tr>
<td><strong>Green</strong></td>
<td>Excellent!</td>
</tr>
<tr>
<td><strong>Tiny</strong></td>
<td>Excellent!</td>
</tr>
<tr>
<td><strong>Huge</strong></td>
<td>Excellent!</td>
</tr>
<tr>
<td><strong>No suggestions</strong></td>
<td>Excellent!</td>
</tr>
<tr>
<td><strong>Text-only</strong></td>
<td>Excellent!</td>
</tr>
</tbody>
</table>
Bunny Condition

A strong password helps prevent unauthorized access to your email account. The stronger your password, the faster Bugs Bunny dances!

Type new password: 

8-character minimum; case sensitive

Password strength: Please enter a password in the box above.

Retype new password: 

Make my password expire every 72 days.

Save
Bunny Condition

A strong password helps prevent unauthorized access to your email account. The stronger your password, the faster Bugs Bunny dances!

Type new password: 

8-character minimum; case sensitive

Password strength: Please enter a password in the box above.

Retype new password: 

Make my password expire every 72 days.

Save
Conditions with Scoring Differences

Type new password: usenIX

8-character minimum; case sensitive

Baseline meter

Fair. Consider adding a digit or making your password longer.

Half-score

Bad. Consider adding a digit or making your password longer.

One-third-score

Bad. Consider adding a digit or making your password longer.

Nudge-B16

Bad. Consider making your password longer.

Nudge-Comp8

Fair. Consider adding a digit or making your password longer.
Conditions with Scoring Differences

Type new password: usenIX$e5
8-character minimum; case sensitive

Baseline meter
Excellent!

Half-score
Poor. Consider adding a different symbol or making your password longer.

One-third-score
Bad. Consider adding a different symbol or making your password longer.

Nudge-B16
Poor. Consider making your password longer.

Nudge-Comp8
Excellent!
Conditions with Scoring Differences

Type new password: usenIX$e5WHYis
8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Fair. Consider adding a different symbol or making your password longer.

One-third-score

Poor. Consider adding a different symbol or making your password longer.

Nudge-B16

Good. Consider making your password longer.

Nudge-Comp8

Excellent!
Conditions with Scoring Differences

Type new password: usenIX$e5WHYismyP4$$
8-character minimum; case sensitive

Baseline meter: Excellent!

Half-score: Good. Consider adding a different symbol or making your password longer.

One-third-score: Poor. Consider adding a different symbol or making your password longer.

Nudge-B16: Excellent.

Nudge-Comp8: Excellent!
Conditions with Scoring Differences

Type new password: usenIX$e5WHYismyP4$$word99
8-character minimum; case sensitive

Baseline meter
Excellent!

Half-score
Excellent!

One-third-score
Fair. Consider adding a different symbol or making your password longer.

Nudge-B16
Excellent.

Nudge-Comp8
Excellent!
Conditions with Scoring Differences

<table>
<thead>
<tr>
<th>Condition</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type new password</td>
<td><code>usenIX$e5WHYismyP4$word99notGOOD</code></td>
</tr>
<tr>
<td>8-character minimum; case sensitive</td>
<td></td>
</tr>
<tr>
<td>Baseline meter</td>
<td>Excellent!</td>
</tr>
<tr>
<td>Half-score</td>
<td>Excellent!</td>
</tr>
<tr>
<td>One-third-score</td>
<td>Fair. Consider making your password longer.</td>
</tr>
<tr>
<td>Nudge-B16</td>
<td>Excellent.</td>
</tr>
<tr>
<td>Nudge-Comp8</td>
<td>Excellent!</td>
</tr>
</tbody>
</table>
Conditions with Scoring Differences

Type new password: 

usenIX$e5WHYismyP4$word99notGOODenough?

8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Excellent!

One-third-score

Excellent!

Nudge-B16

Excellent.

Nudge-Comp8

Excellent!
Password Meters (Scoring)

<table>
<thead>
<tr>
<th>Percentage of Passwords Cracked</th>
<th>Number of Guesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>$10^4$</td>
</tr>
<tr>
<td>10%</td>
<td>$10^5$</td>
</tr>
<tr>
<td>20%</td>
<td>$10^6$</td>
</tr>
<tr>
<td>30%</td>
<td>$10^7$</td>
</tr>
<tr>
<td>40%</td>
<td>$10^8$</td>
</tr>
<tr>
<td>50%</td>
<td>$10^9$</td>
</tr>
</tbody>
</table>

- **Weak**: $5 \times 10^8$
- **Medium**: $5 \times 10^{10}$
- **Strong**: $5 \times 10^{12}$

- No meter
- Baseline meter
- Nudge-comp8
- Bold text-only half
- Text-only half
- Nudge-16
- One-third-score
- Half-score
Password Meters (Scoring)

<table>
<thead>
<tr>
<th>Number of Guesses</th>
<th>Percentage of Passwords Cracked</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>10</td>
<td>10%</td>
</tr>
<tr>
<td>20</td>
<td>20%</td>
</tr>
<tr>
<td>30</td>
<td>30%</td>
</tr>
<tr>
<td>40</td>
<td>40%</td>
</tr>
<tr>
<td>50</td>
<td>50%</td>
</tr>
<tr>
<td>60</td>
<td>60%</td>
</tr>
<tr>
<td>70</td>
<td>70%</td>
</tr>
<tr>
<td>80</td>
<td>80%</td>
</tr>
<tr>
<td>90</td>
<td>90%</td>
</tr>
<tr>
<td>100</td>
<td>100%</td>
</tr>
</tbody>
</table>

No meter
Baseline meter
Nudge
Bold text - only
Half-text
- only half
Nudge
One-third-score
Half-score

Stringent meters with visual bars increase resistance to guessing, without affecting memorability.

Too stringent can deplete user buy-in and backfire.

Visual changes don’t significantly increase resistance to guessing.