Usable Security

Computer Systems Security - 11/5

Daniel Votipka
Fall 2018

(some slides courtesy of Michelle Mazurek, Lorrie Cranor, Mike Reiter, Rob Reeder, and Blasé Ur)

In today's lecture …

- Key challenges
- How to study usable security
  - Grey, password meters, hackers vs. testers
- Guidelines for making things better

What is usable security?

The Human Threat

“Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations…

The Human Threat

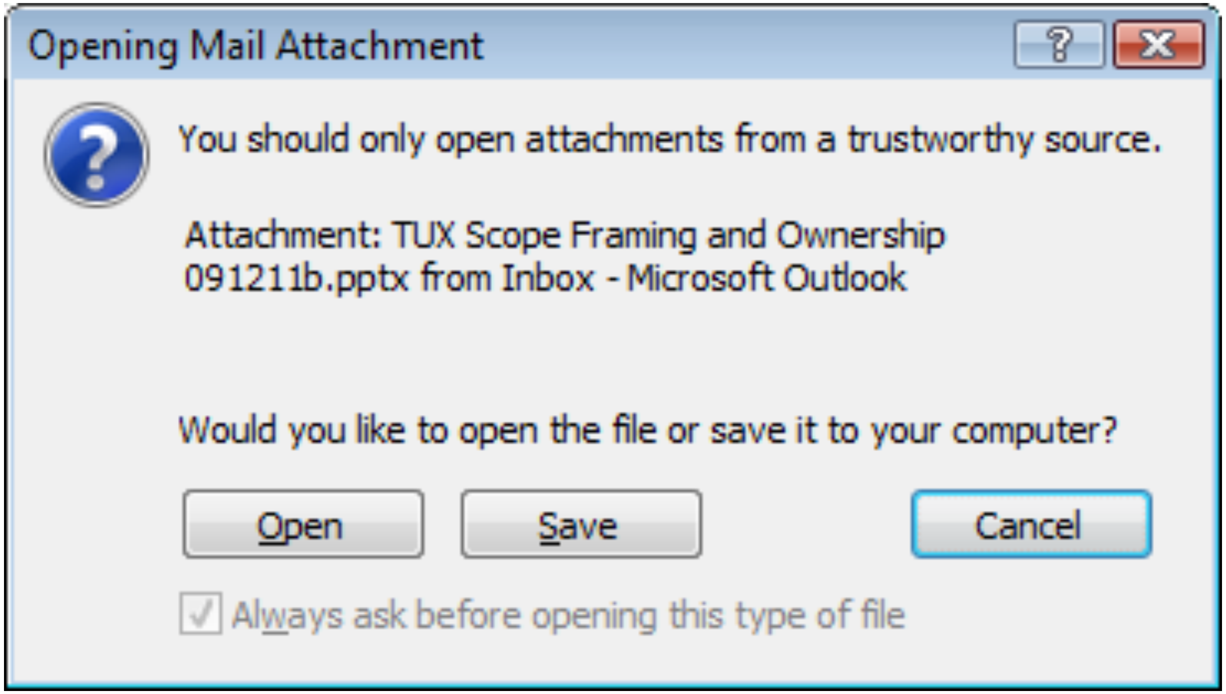
> “Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations…but they are sufficiently pervasive that we must design our protocols around their limitations.”

–– C. Kaufman, R. Perlman, and M. Speciner.
Network Security: PRIVATE Communication in a PUBLIC World.
2nd edition. Prentice Hall, page 237, 2002.

Key challenges

Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing

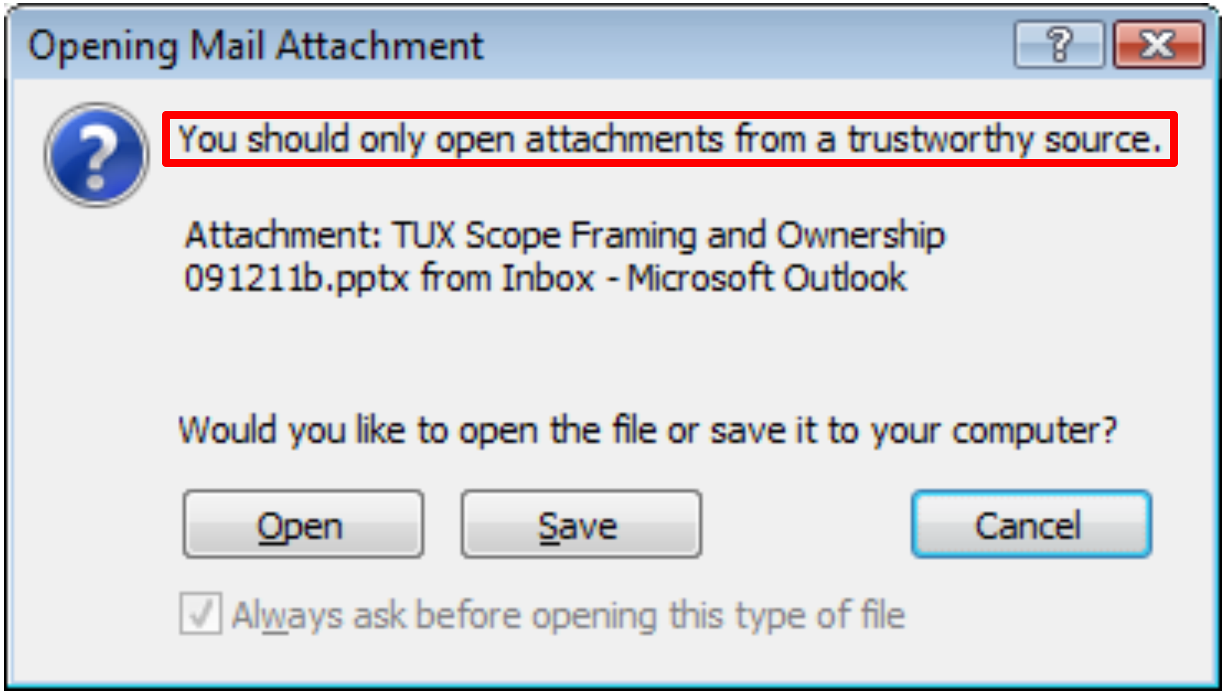


You should only open attachments from a trustworthy source.

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?

☑ Always ask before opening this type of file



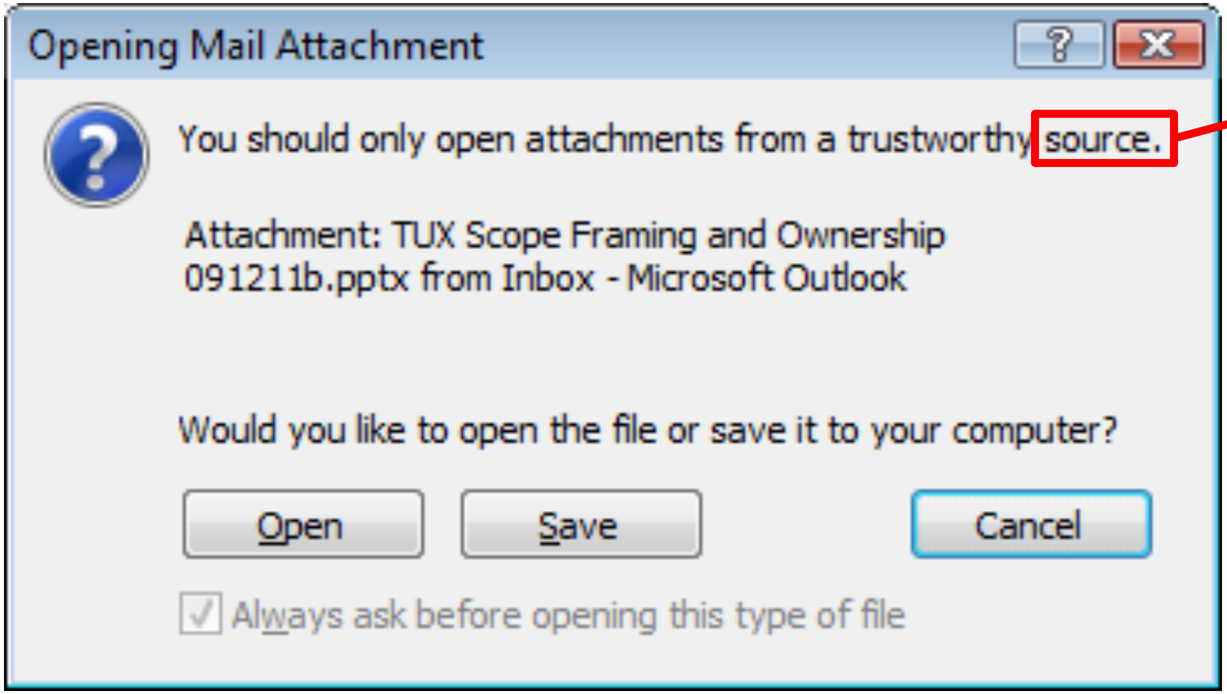
Opening Mail Attachment

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?

☑ Always ask before opening this type of file



Opening Mail Attachment

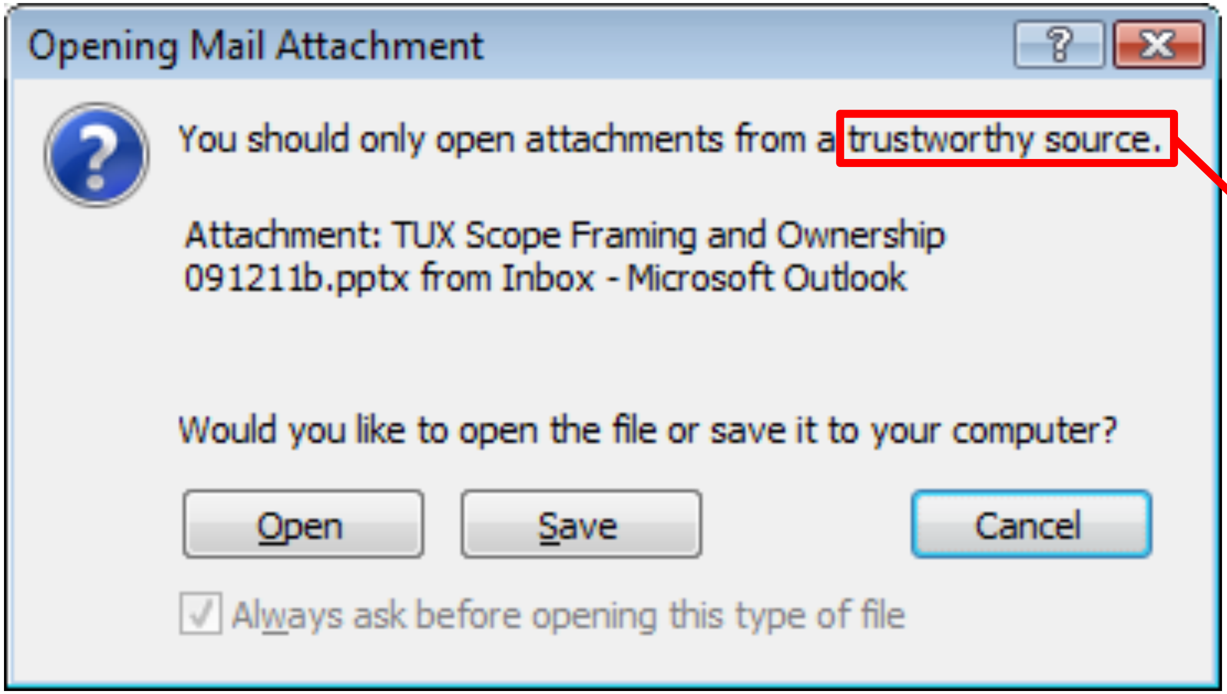
You should only open attachments from a trustworthy source.

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?

☑ Always ask before opening this type of file

What's the source of this attachment?



Opening Mail Attachment

You should only open attachments from a trustworthy source.

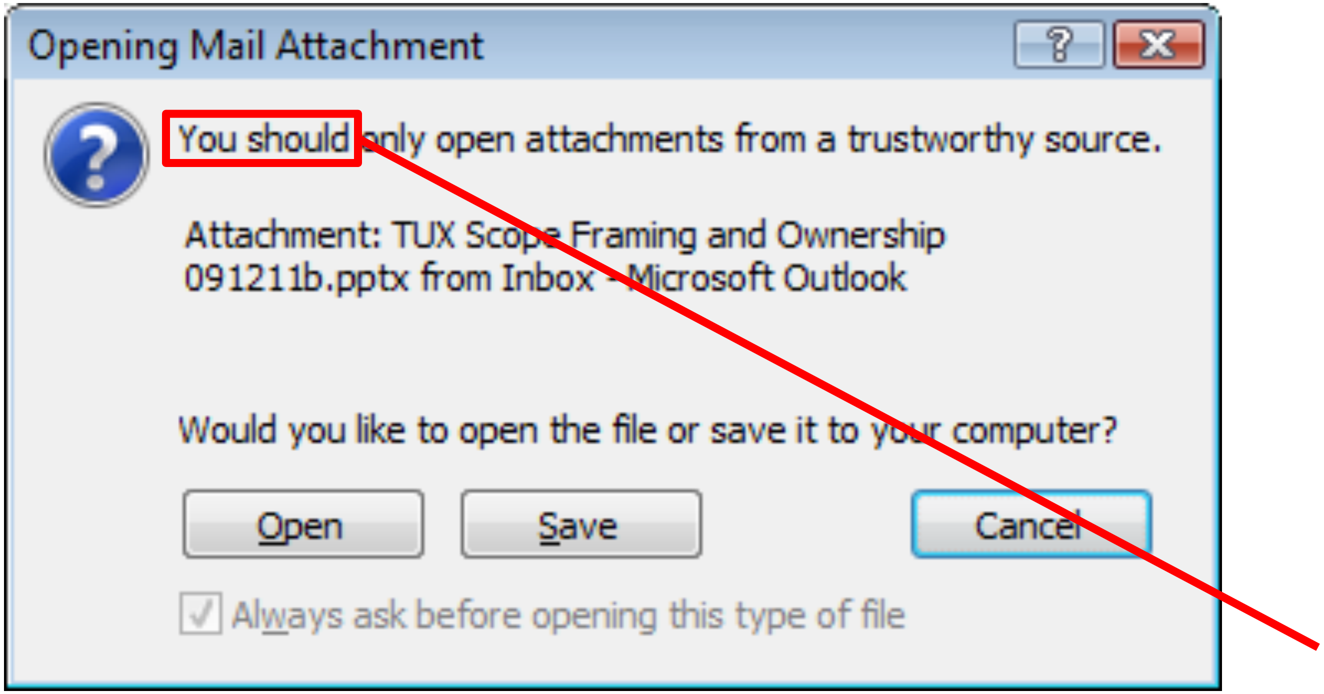
Attachment: TUX Scope Framing and Ownership 091211b.pptx from Inbox - Microsoft Outlook

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

☑ Always ask before opening this type of file

What's the source of this attachment?

What makes a source trustworthy or not trustworthy?



Opening Mail Attachment

You should only open attachments from a trustworthy source.

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

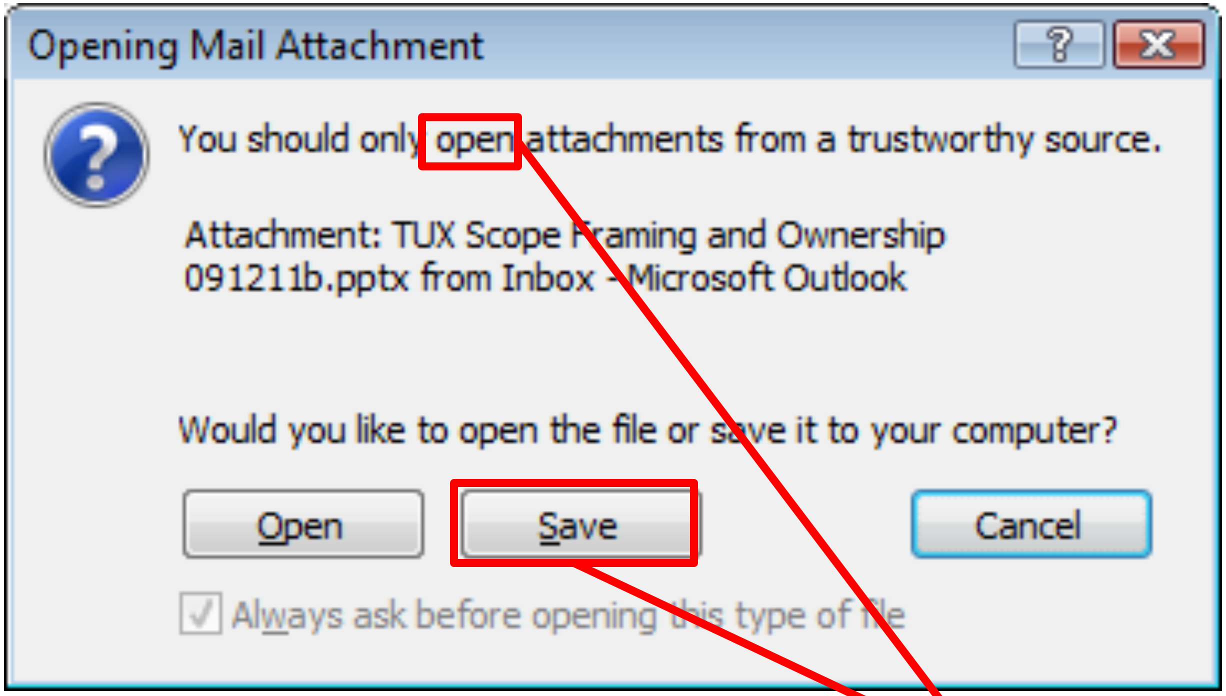
Would you like to open the file or save it to your computer?

☑ Always ask before opening this type of file

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?



Opening Mail Attachment

You should only open attachments from a trustworthy source.

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

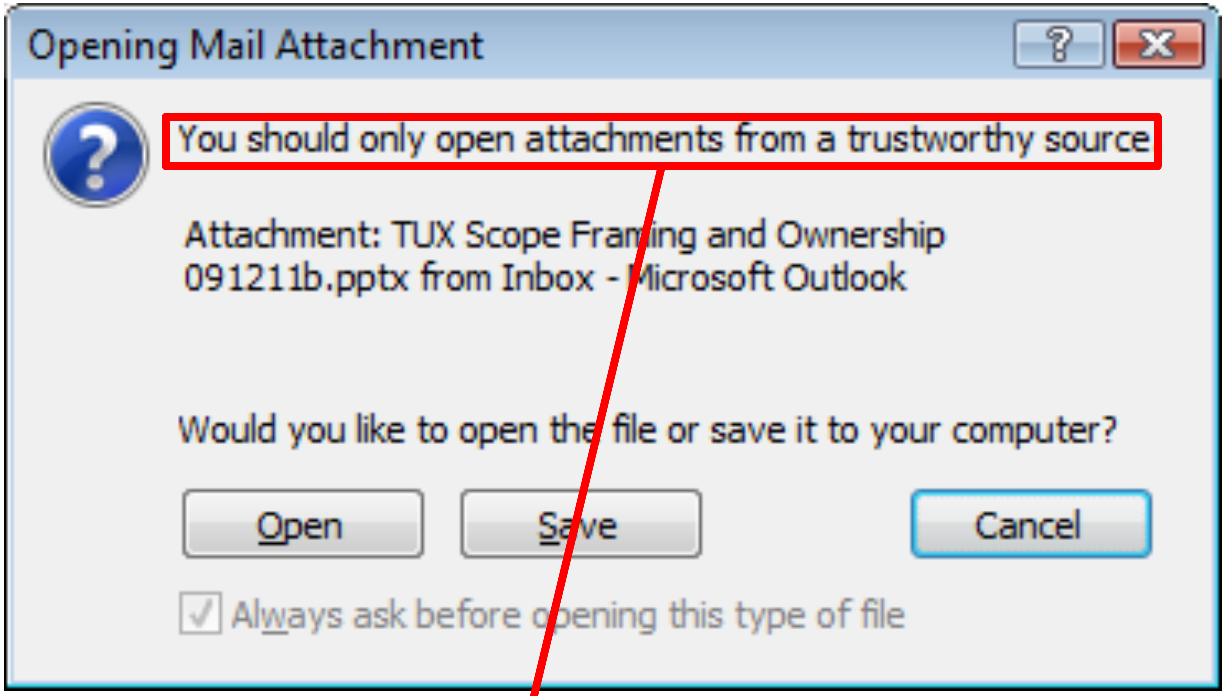
Would you like to open the file or save it to your computer?

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?



Opening Mail Attachment

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?

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?

Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing

Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Security is a secondary task
  - Users are trying to get something else done

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

Good security practices

- 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

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

Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Security is a secondary task
  - Users are trying to get something else done

Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Security is a secondary task
  - Users are trying to get something else done
- Human capabilities are limited

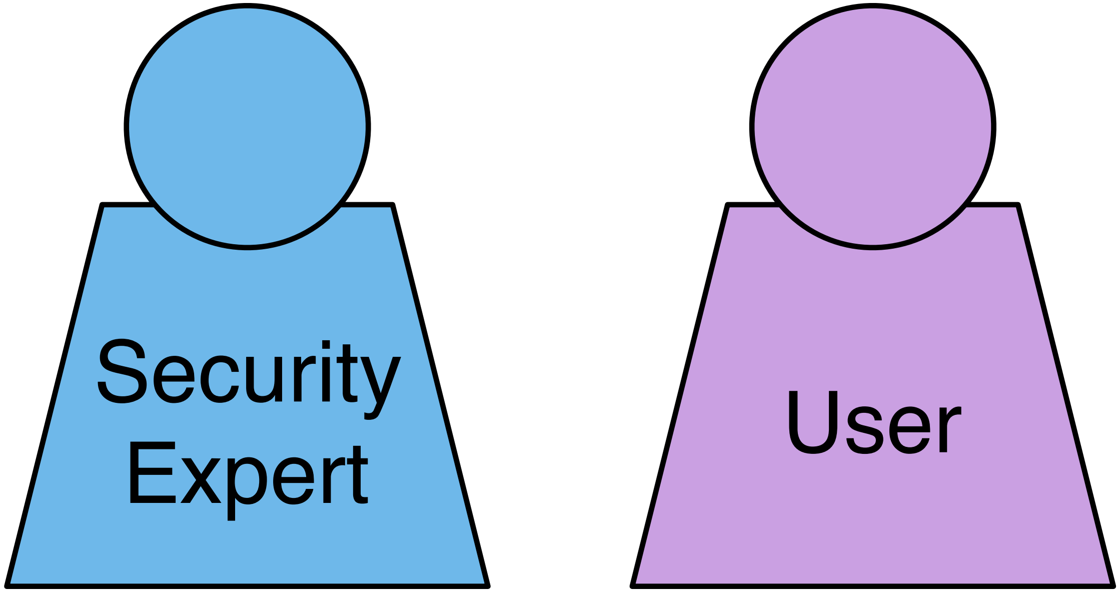
Are you capable of remembering a unique strong password for every account you have?

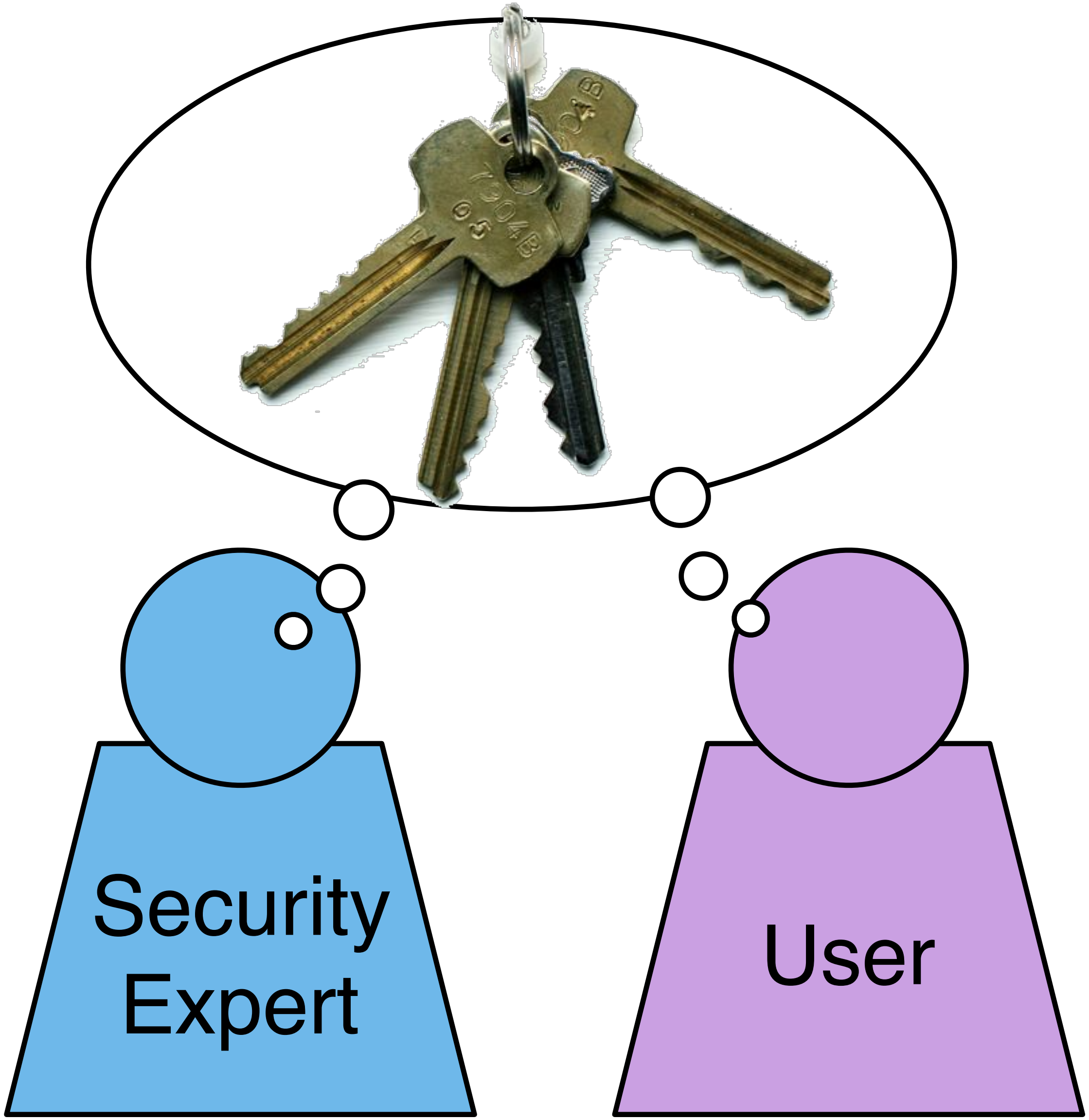
Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Security is a secondary task
  - Users are trying to get something else done
- Human capabilities are limited

Key challenges

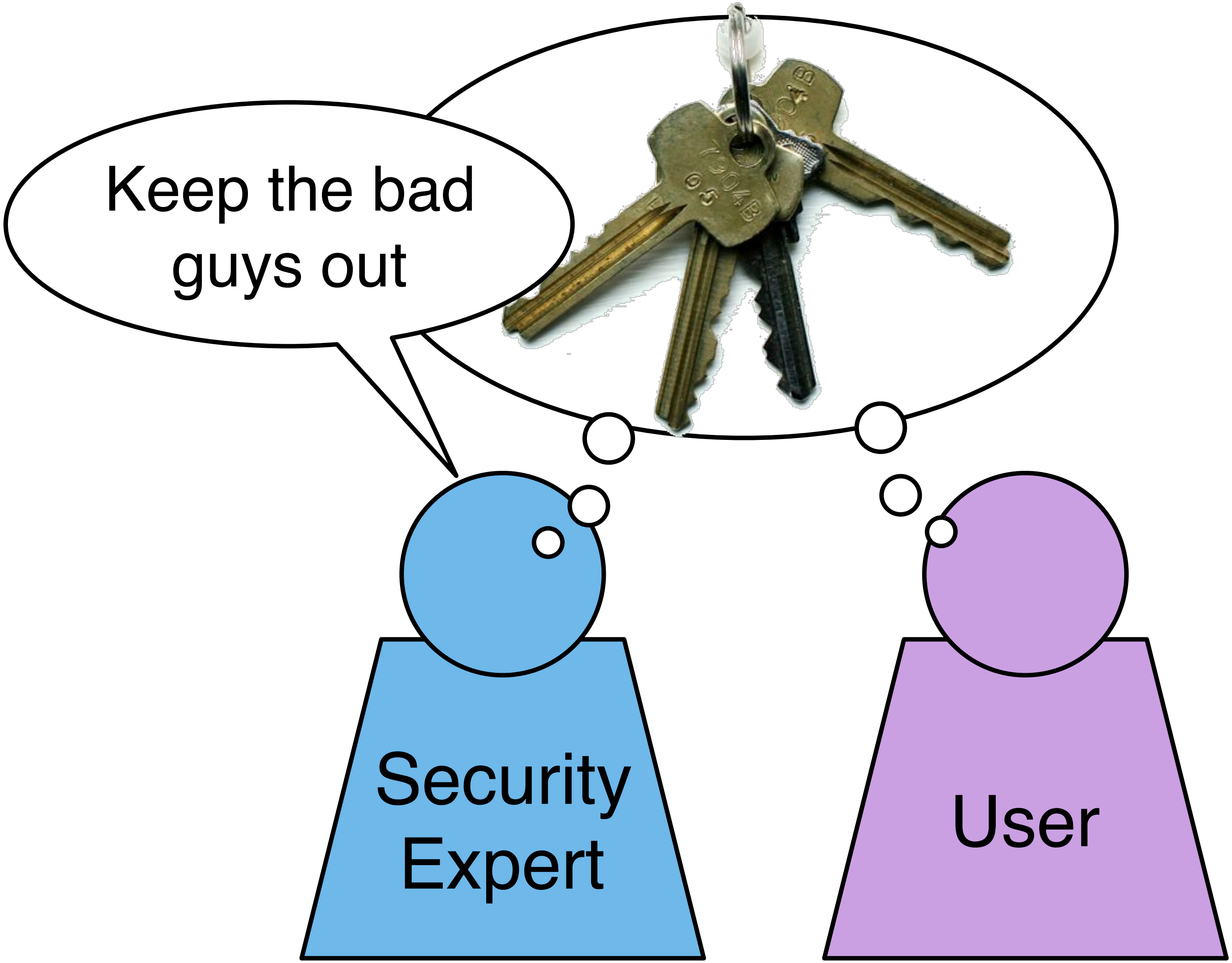
- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Security is a secondary task
  - Users are trying to get something else done
- Human capabilities are limited
- Misaligned priorities


Security Expert
User



Security Expert

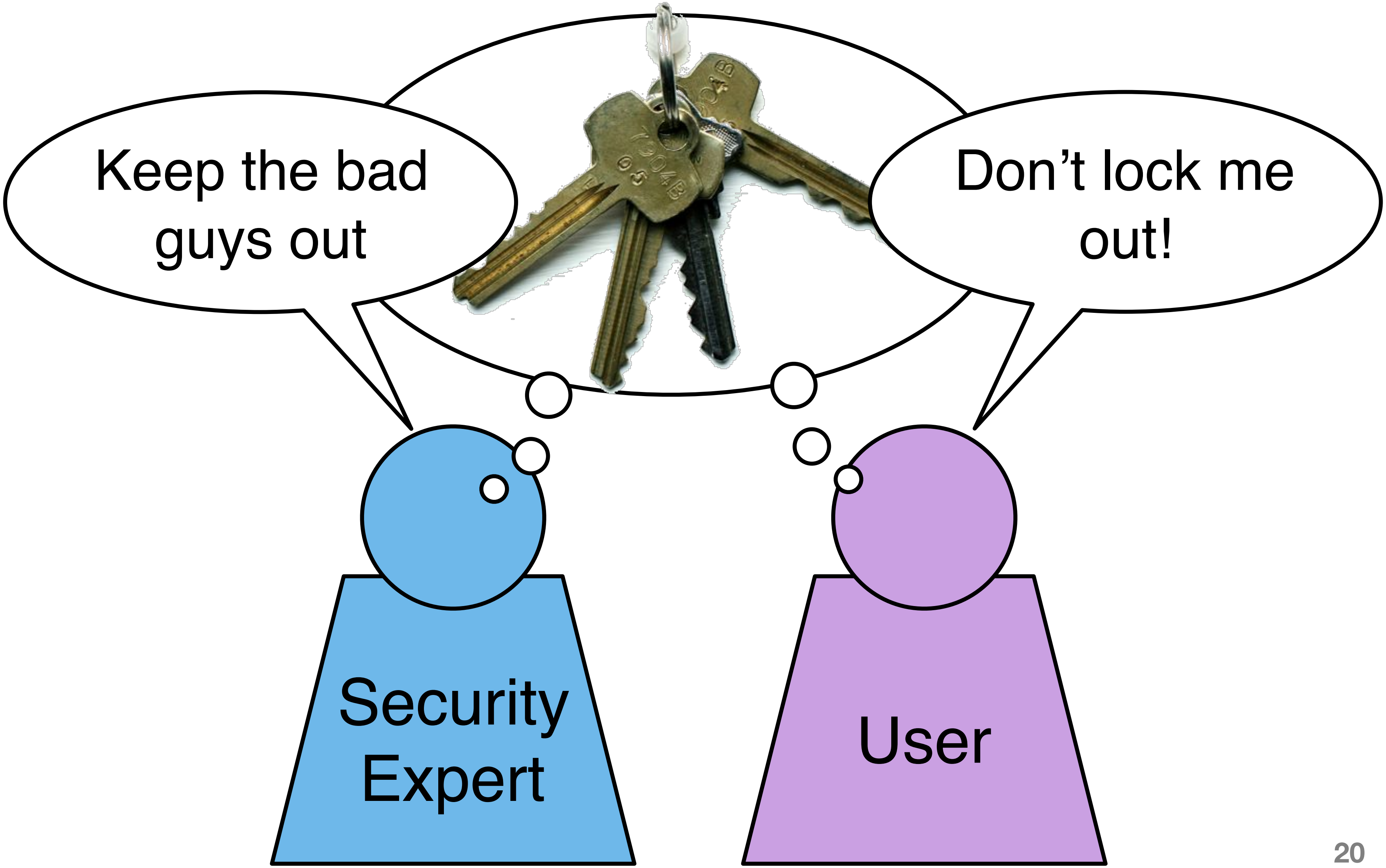
User



Keep the bad guys out

Security Expert

User



Keep the bad guys out

Don’t lock me out!

Security Expert

User

Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Security is a secondary task
  - Users are trying to get something else done
- Human capabilities are limited
- Misaligned priorities

Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Security is a secondary task
  - Users are trying to get something else done
- Human capabilities are limited
- Misaligned priorities
- Habituation
  - Active adversaries (Unlike ordinary UX)

Habituation

“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.”

Habituation

"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

Exercise: Draw a penny

No cheating!

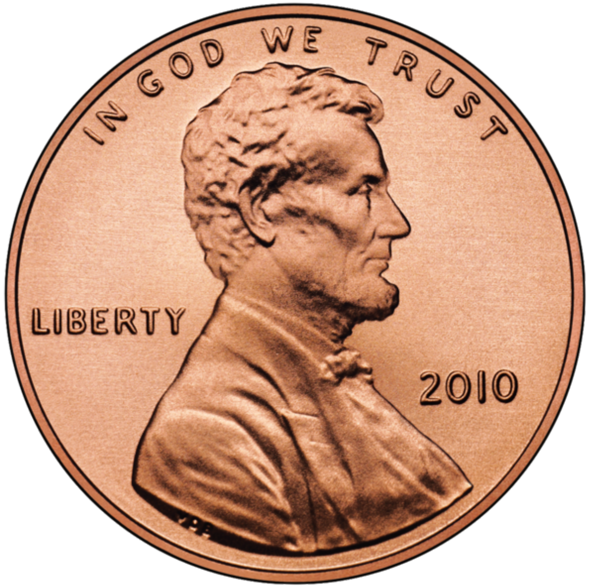
- Draw a circle
- Sketch the layout of the four basic items on the front of a US penny
  - What are the items, and how are they positioned?

Exercise: Draw a penny

No cheating!

- 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

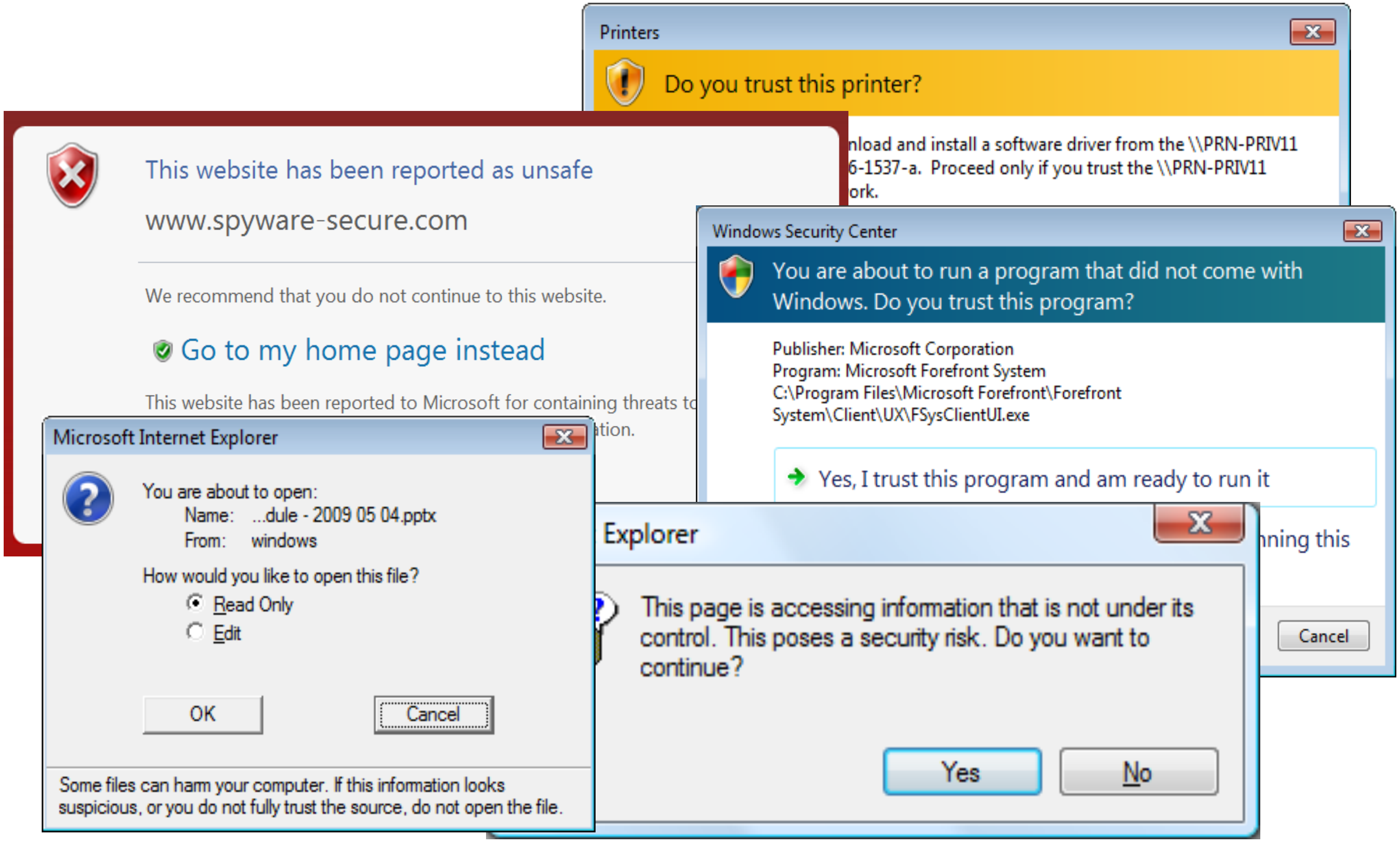


- Score:
  - 1 for Abraham Lincoln
  - +1 for Abraham Lincoln facing right
  - +1 for "Liberty"
  - +1 for "Liberty" to Abe's left
  - +1 for "In God We Trust"
  - +1 for "In God We Trust" over Abe's head
  - +1 for the year
  - +1 for the year to Abe's right
  - Extra credit: +1 for the mint letter 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



Printers

Do you trust this printer?

nload and install a software driver from the \\PRN-PRIV11
6-1537-a. Proceed only if you trust the \\PRN-PRIV11
ork.

This website has been reported as unsafe

www.spyware-secure.com

We recommend that you do not continue to this website.

Go to my home page instead

This website has been reported to Microsoft for containing threats to
ation.

Windows Security Center

You are about to run a program that did not come with Windows. Do you trust this program?

Publisher: Microsoft Corporation
Program: Microsoft Forefront System
C:\Program Files\Microsoft Forefront\Forefront System\Client\UX\FSysClientUI.exe

Yes, I trust this program and am ready to run it

nning this

Microsoft Internet Explorer

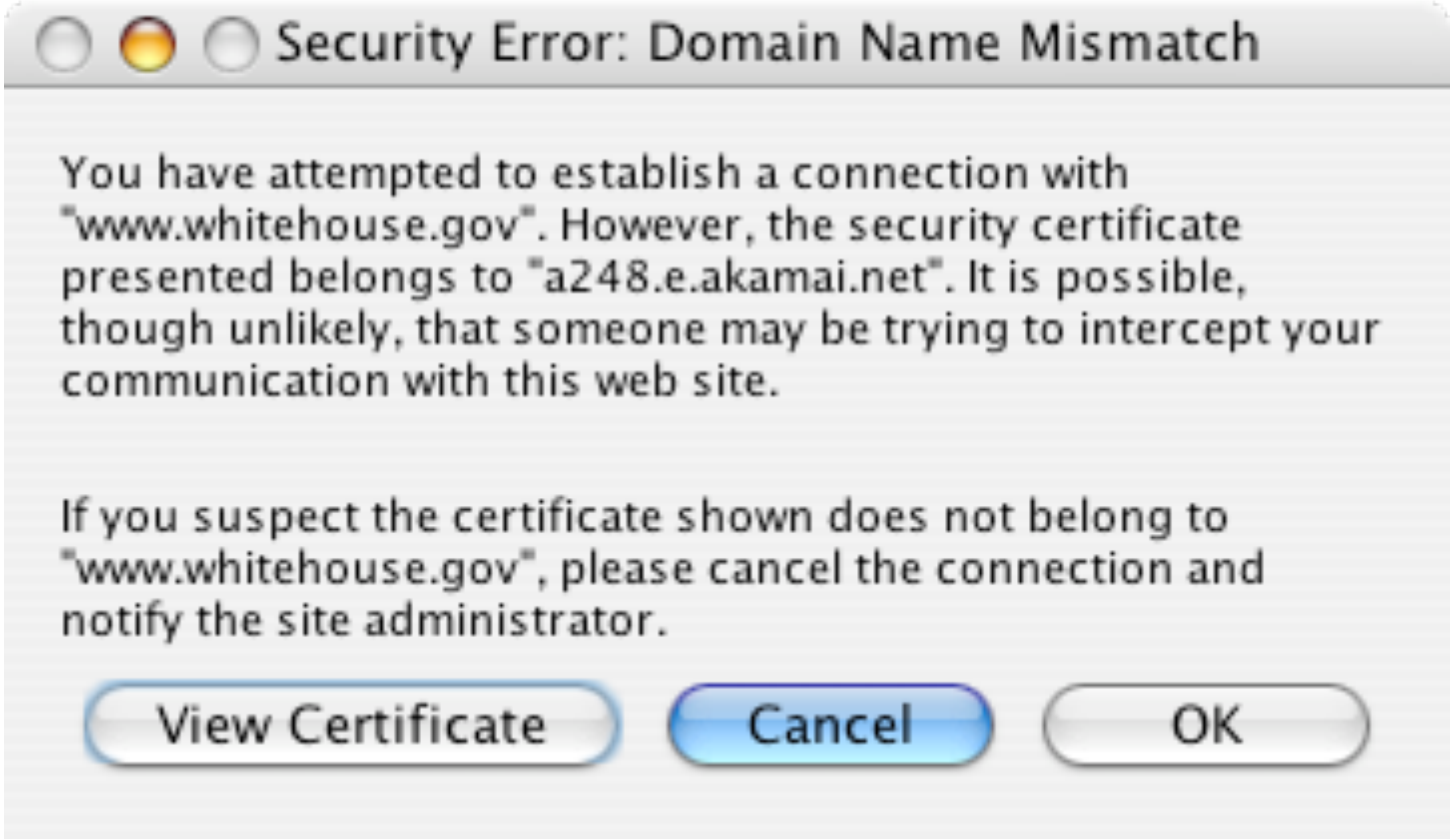
You are about to open:
Name: ...dule - 2009 05 04.pptx
From: windows

How would you like to open this file?
● Read Only
○ Edit

Some files can harm your computer. If this information looks suspicious, or you do not fully trust the source, do not open the file.

Explorer

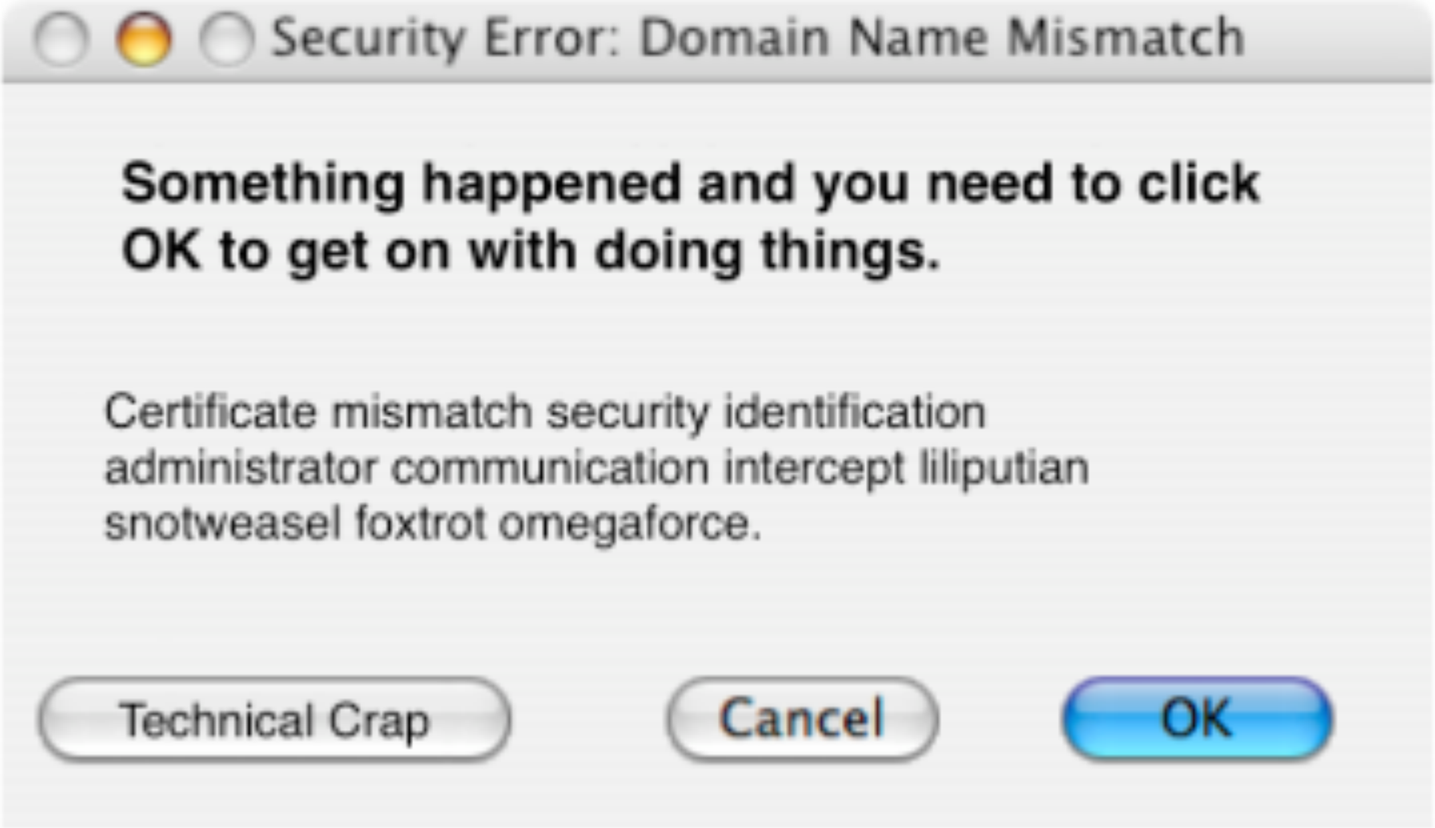
This page is accessing information that is not under its control. This poses a security risk. Do you want to continue?



Security Error: Domain Name Mismatch

You have attempted to establish a connection with "www.whitehouse.gov". However, the security certificate presented belongs to "a248.e.akamai.net". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.

If you suspect the certificate shown does not belong to "www.whitehouse.gov", please cancel the connection and notify the site administrator.



Security Error: Domain Name Mismatch

Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegaforce.

Image courtesy of Johnathan Nightingale

Key challenges

- Security concepts are hard
  - Viruses, certificates, SSL, encryption, phishing
- Security is a secondary task
  - Users are trying to get something else done
- Human capabilities are limited
- Misaligned priorities
- Habituation
  - Active adversaries (Unlike ordinary UX)

How can we test if our system is usable?

Case Study #1: Grey and user Buy-in

https://www.archive.ece.cmu.edu/~lbauer/papers/2007/soups2007.pdf

Is Grey too slow?

- Grey: Smartphone-based access control
  - Strong security benefits vs. keys
- Users complained about speed

[Bauer et. al, SOUPS 2007]

Is Grey too slow?

- Grey: Smartphone-based access control
  - Strong security benefits vs. keys
- Users complained about speed
  - Videotaped doors to measure Grey vs. keys

[Bauer et. al, SOUPS 2007]

Is Grey too slow?

- Grey: Smartphone-based access control
  - Strong security benefits vs. keys
- Users complained about speed
  - Videotaped doors to measure Grey vs. keys
  - Monitored access/use logs

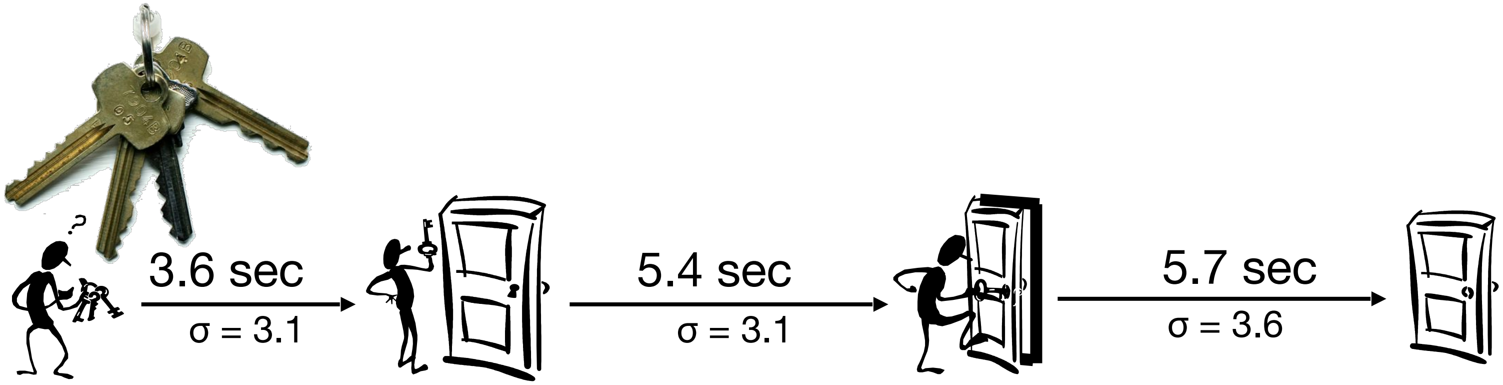
[Bauer et. al, SOUPS 2007]

Is Grey too slow?

- Grey: Smartphone-based access control
  - Strong security benefits vs. keys
- Users complained about speed
  - Videotaped doors to measure Grey vs. keys
  - Monitored access/use logs
  - Periodically asked Grey users to discuss their experience using it

[Bauer et. al, SOUPS 2007]

Average access times



Getting keys

3.6 sec

σ = 3.1

Stop in front of door

5.4 sec

σ = 3.1

Door opened

5.7 sec

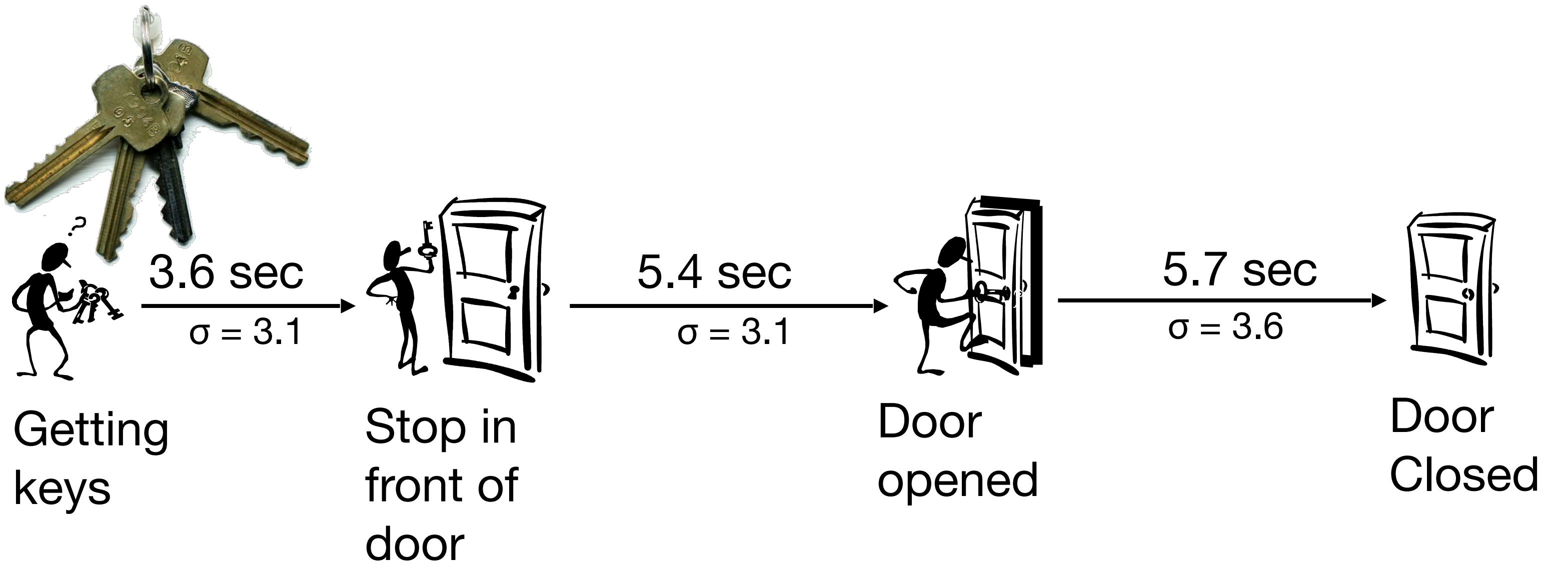
σ = 3.6

Door Closed

Total 14.7 sec

σ = 5.6

Average access times



Getting keys

3.6 sec

σ = 3.1

Stop in front of door

5.4 sec

σ = 3.1

Door opened

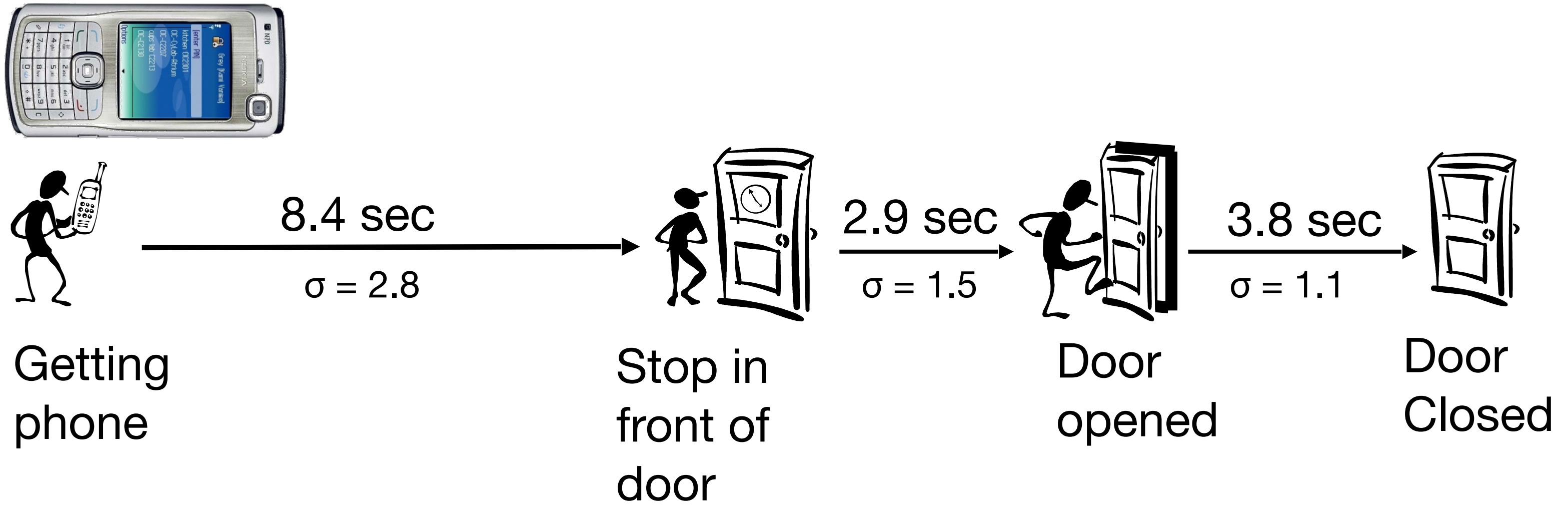
5.7 sec

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

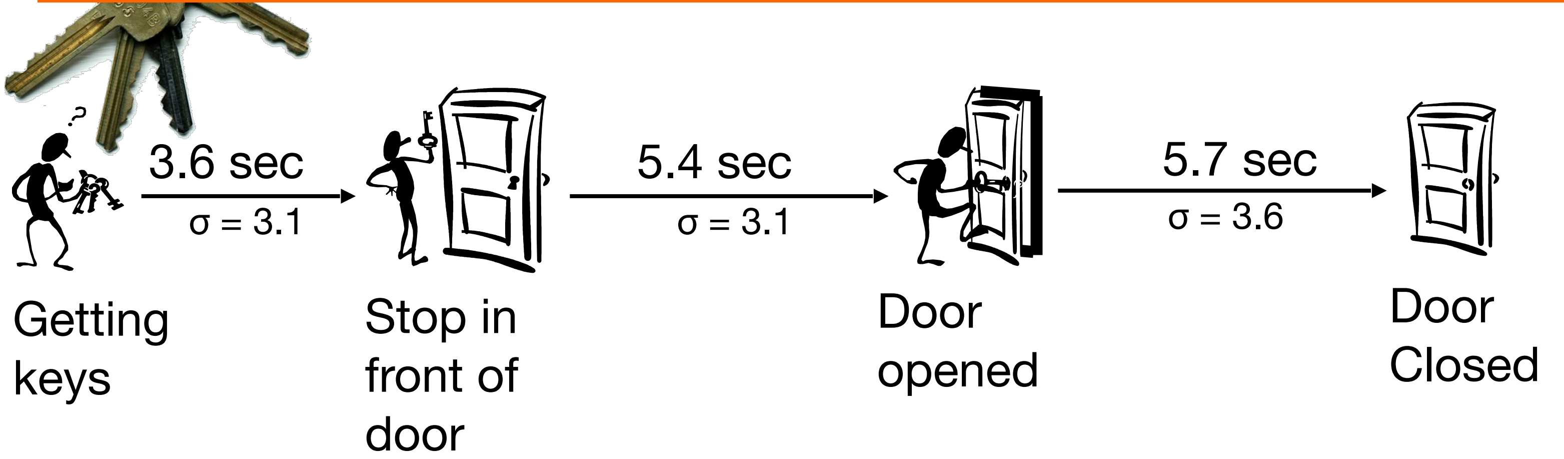
Door Closed

Total 15.1 sec

σ = 3.9

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

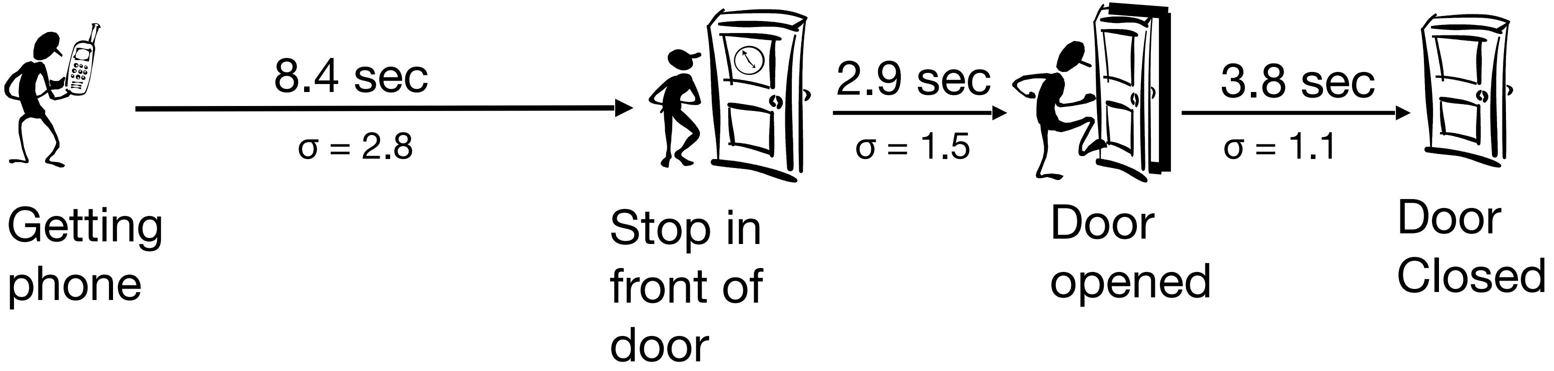
5.7 sec

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

“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.”

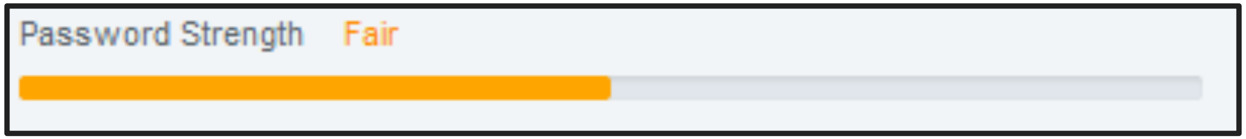
"I find myself standing outside and everybody inside is looking at me standing outside while I am trying to futz with my phone and open the stupid door."

Takeaway: Misaligned priorities

Case Study #2: Password meters and motivating your users

https://www.blaseur.com/papers/sec12_pwmeters_paper.pdf

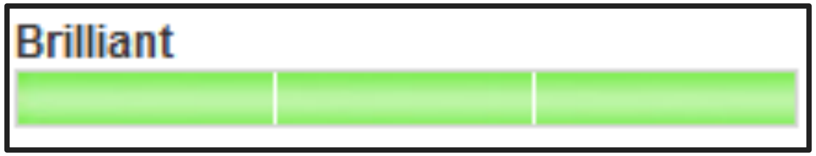
Password Meters …



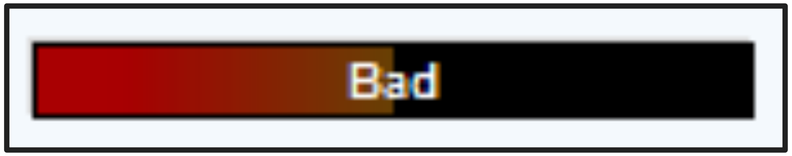
Password Strength Fair

Password Meters …

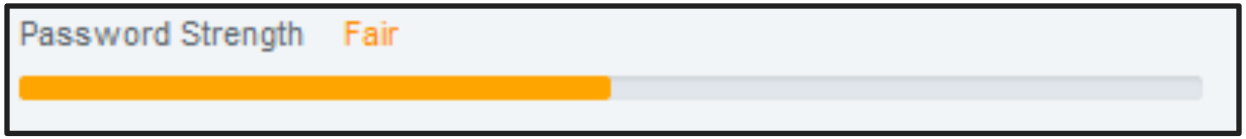
- … come in all shapes and sizes



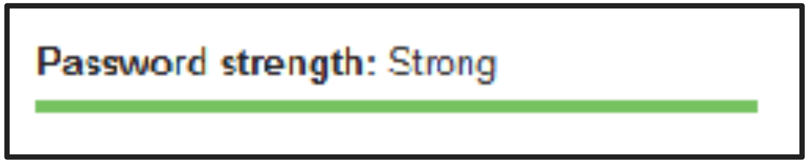
Brilliant



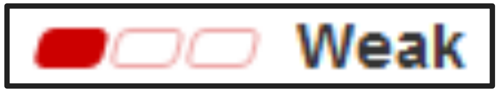
Bad



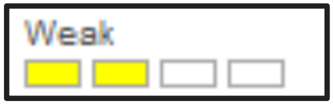
Password Strength Fair



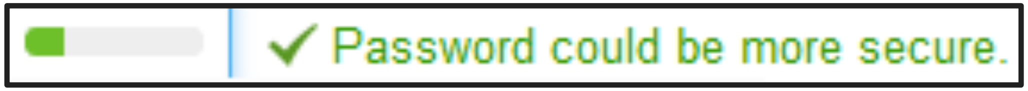
Password strength: Strong



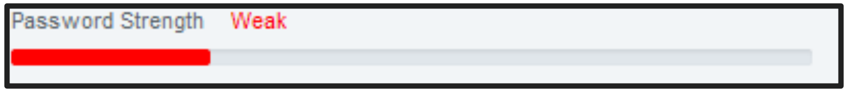
Weak



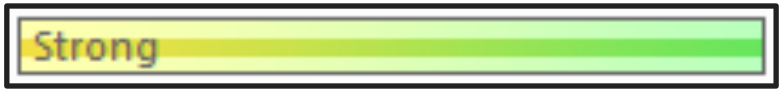
Weak



✓ Password could be more secure.



Password Strength Weak



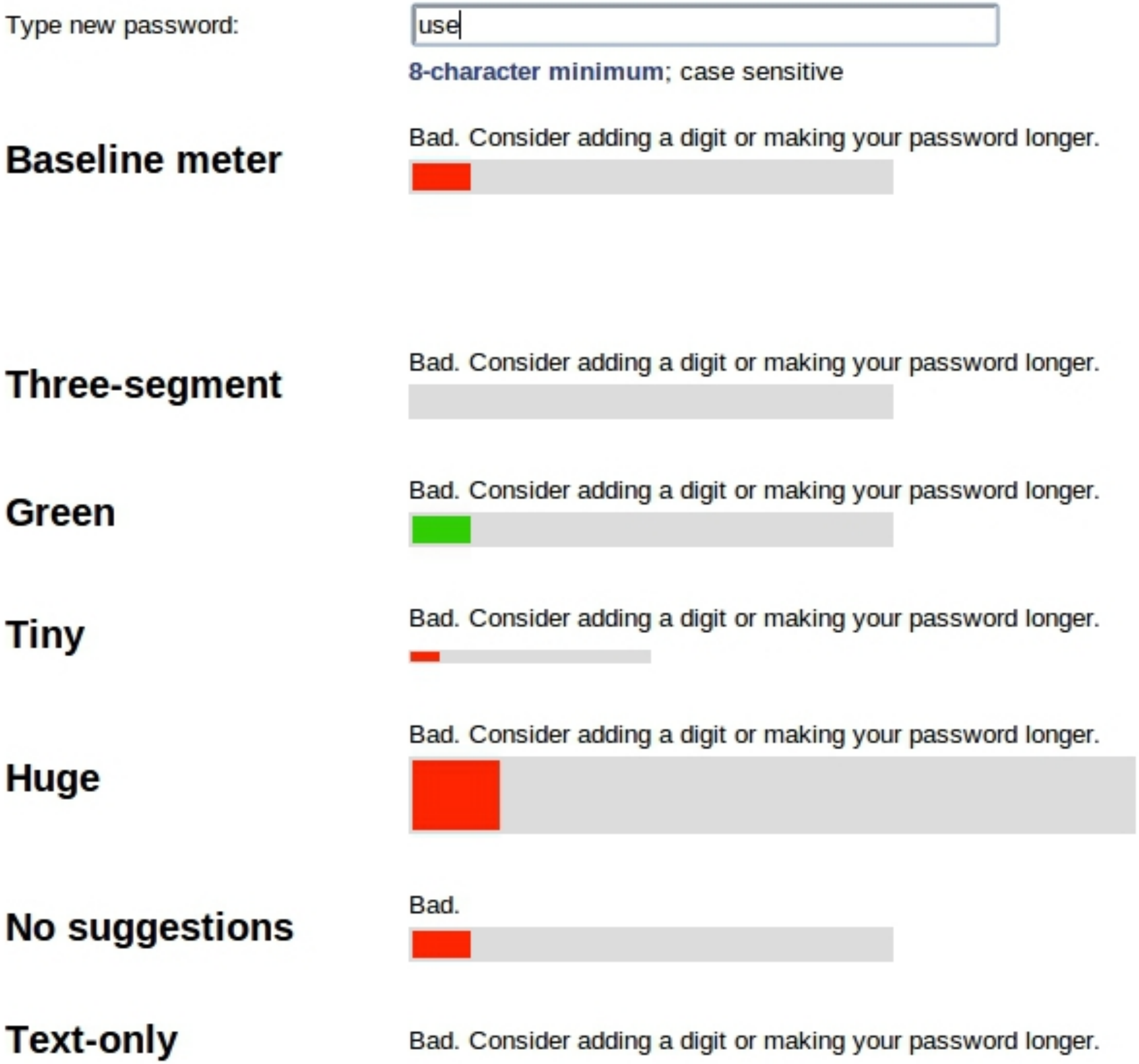
Strong

[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



Type new password: use

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.

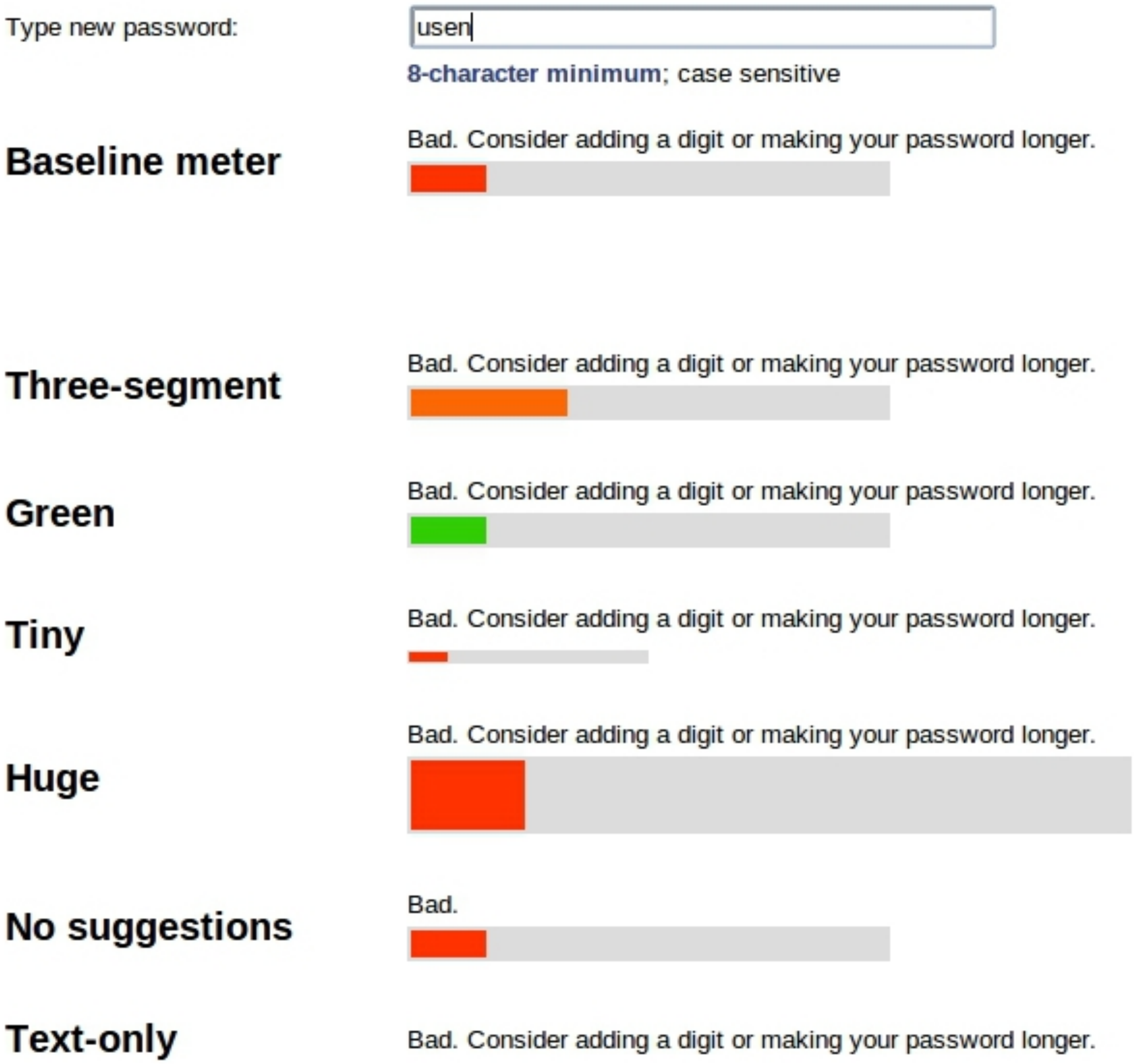
No suggestions

Bad.

Text-only

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

Conditions with Visual Differences



Type new password: usen

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.

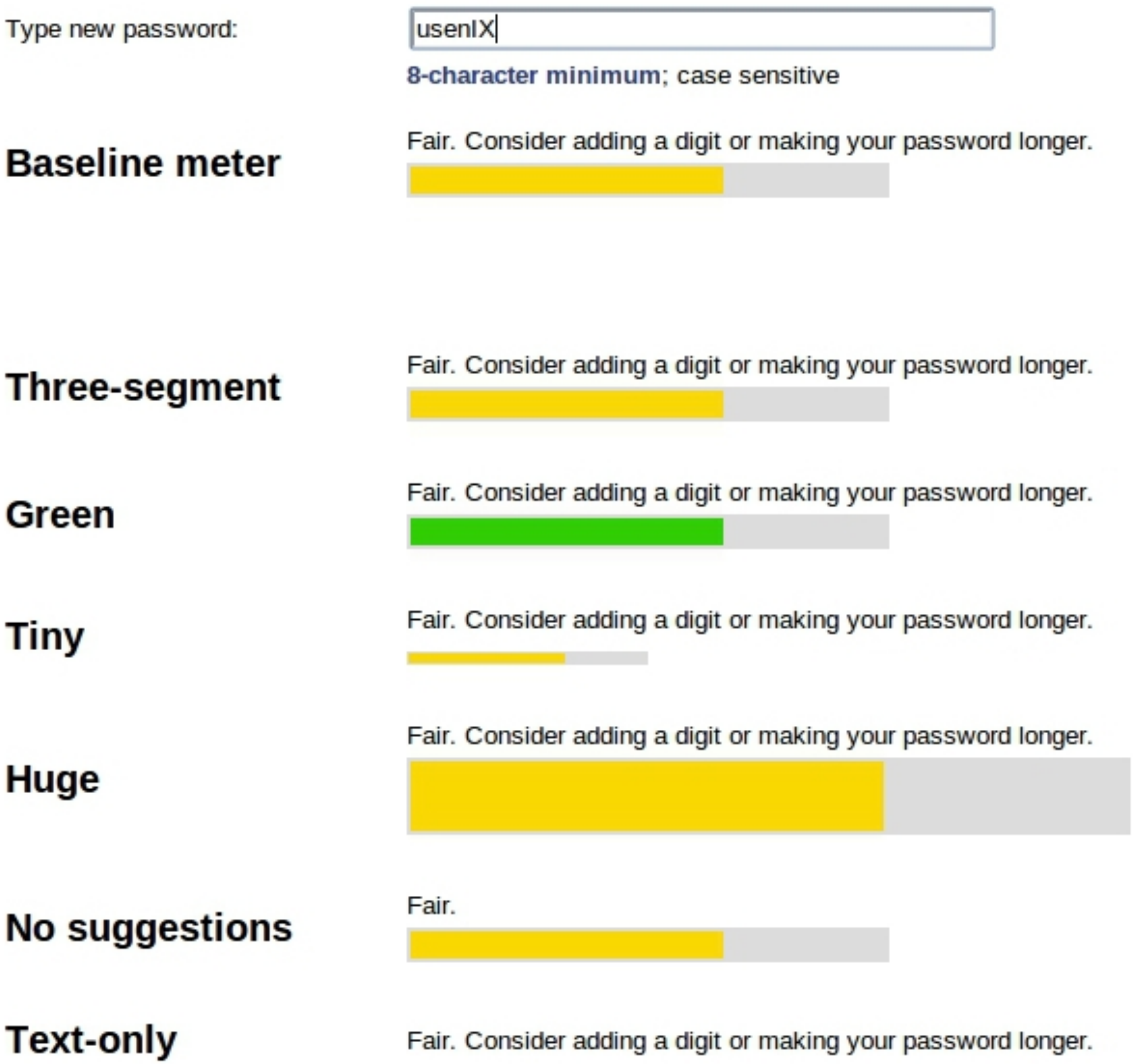
No suggestions

Bad.

Text-only

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

Conditions with Visual Differences



Type new password: usenIX

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.

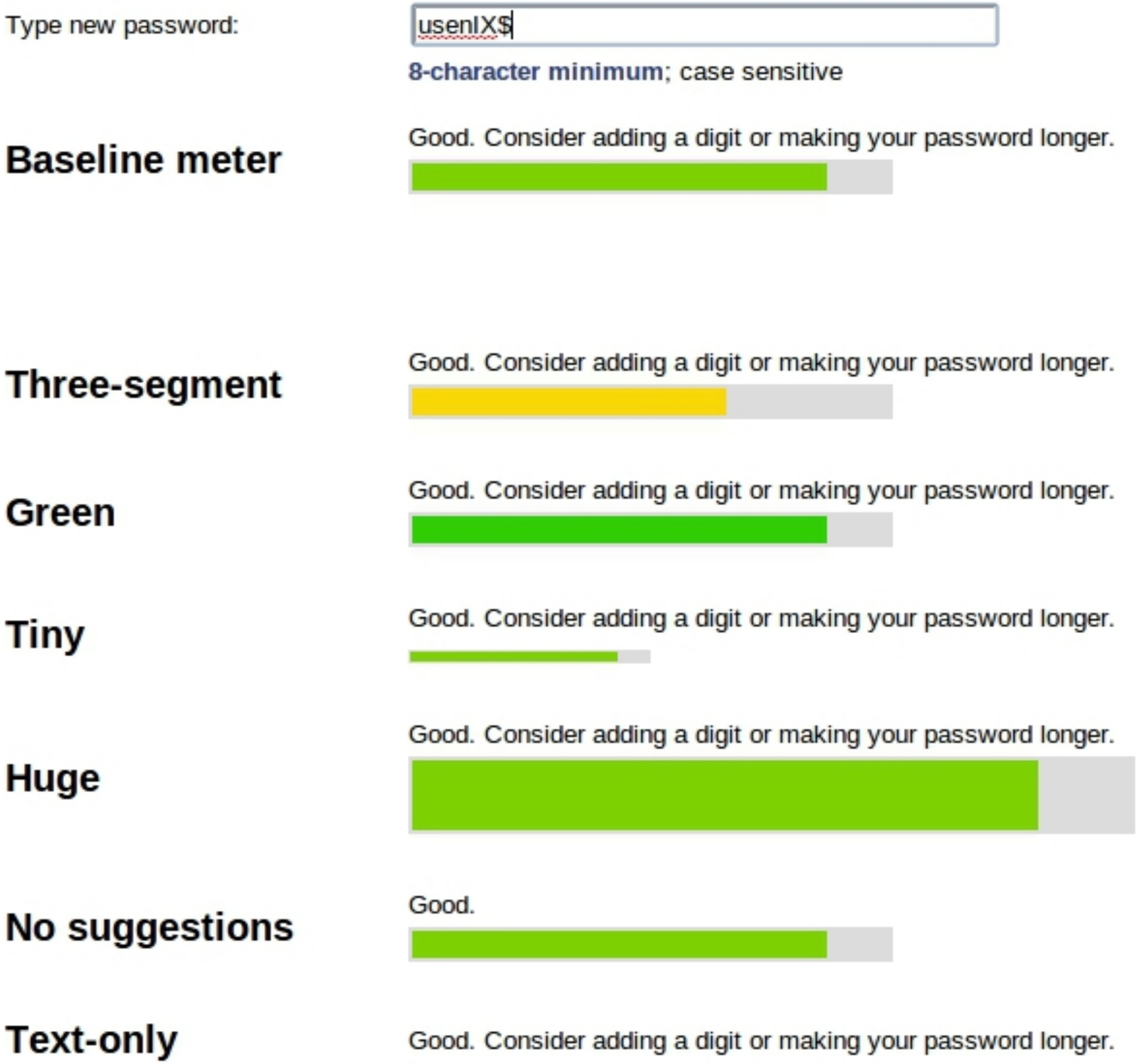
No suggestions

Fair.

Text-only

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

Conditions with Visual Differences



Type new password: usenIX$

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.

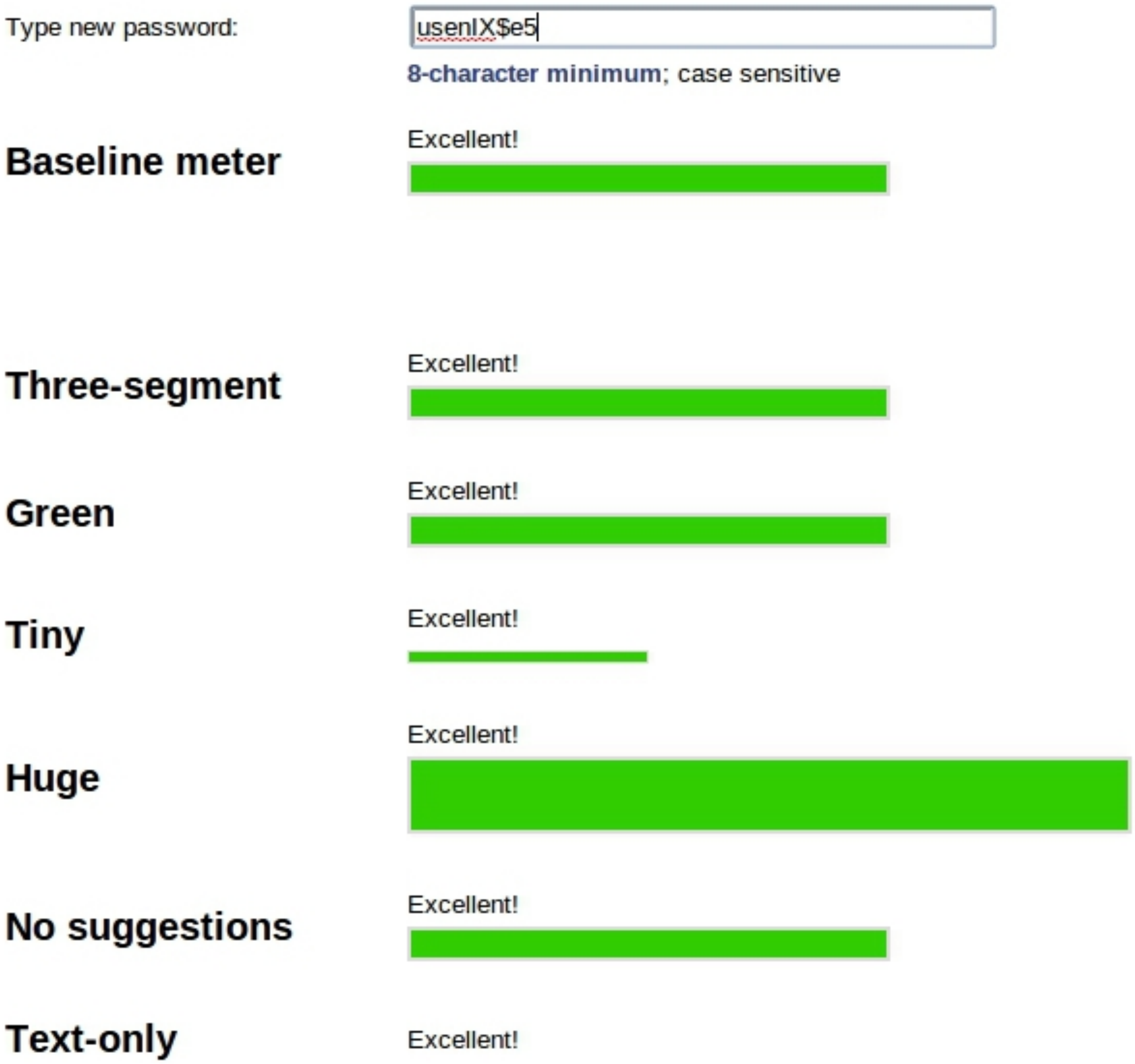
No suggestions

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!

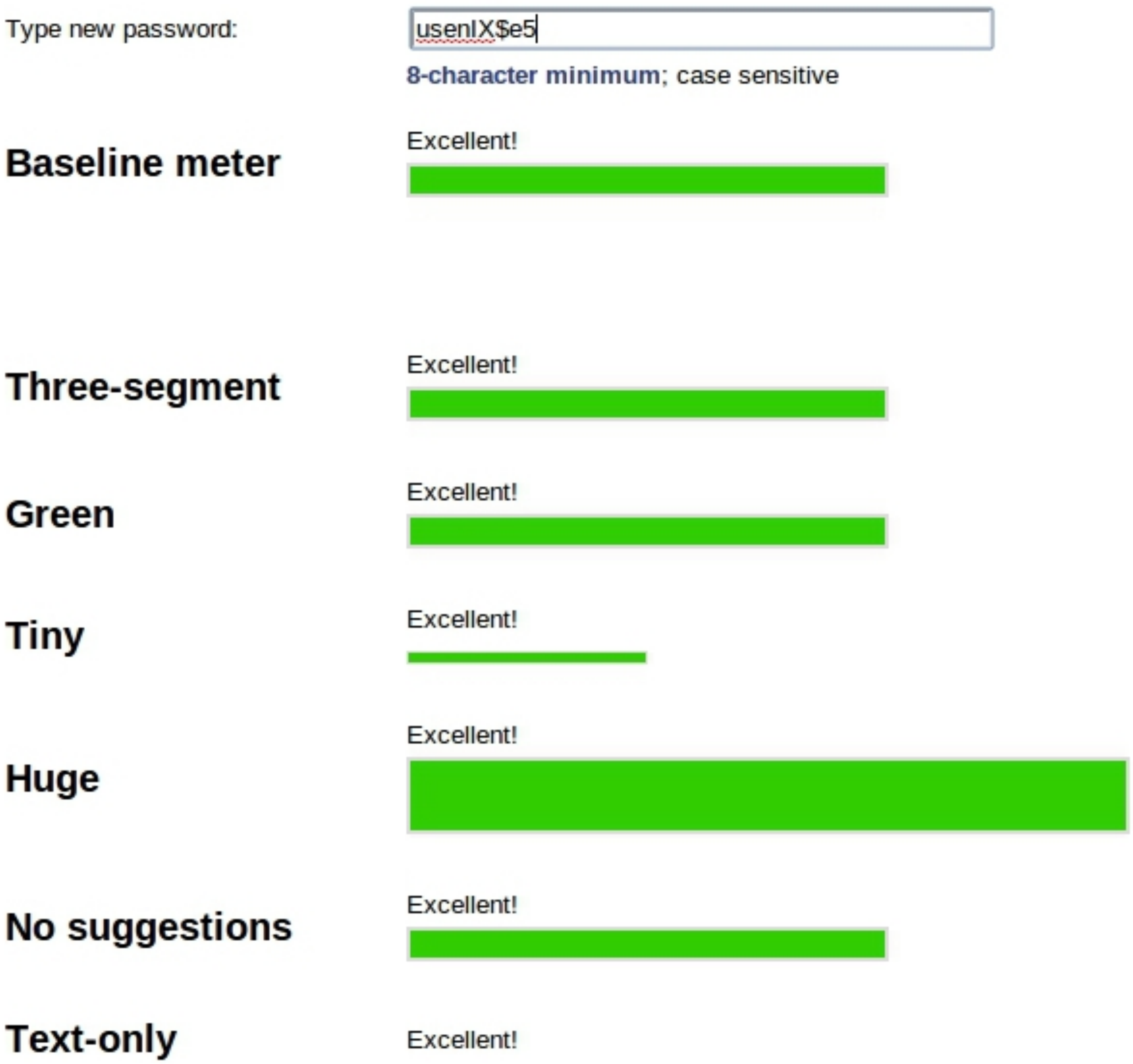
Tiny Excellent!

Huge Excellent!

No suggestions Excellent!

Text-only Excellent!

Conditions with Visual Differences



Type new password: usenIX$e5

8-character minimum; case sensitive

Baseline meter Excellent!

Three-segment Excellent!

Green Excellent!

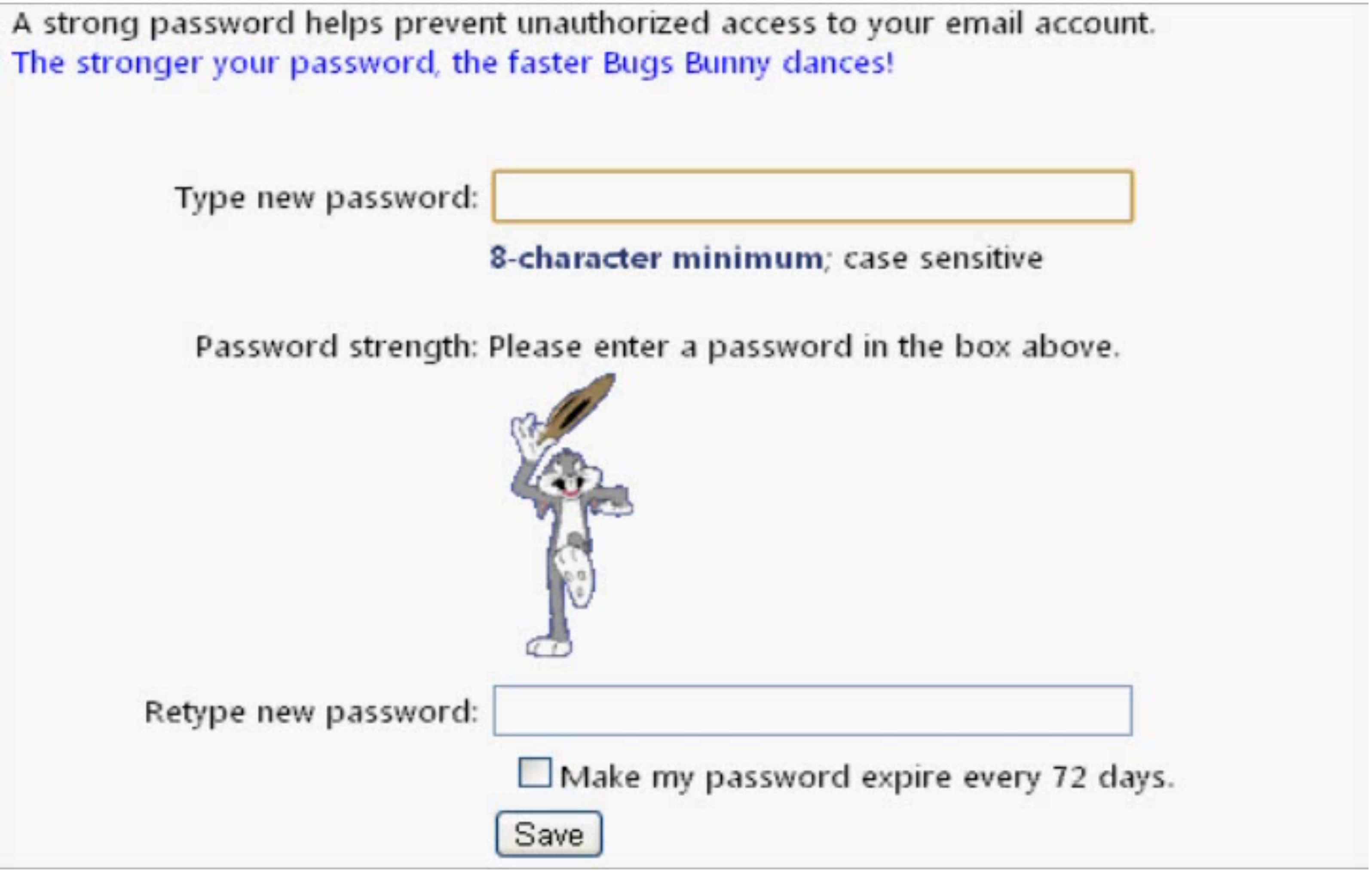
Tiny Excellent!

Huge Excellent!

No suggestions Excellent!

Text-only Excellent!

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:

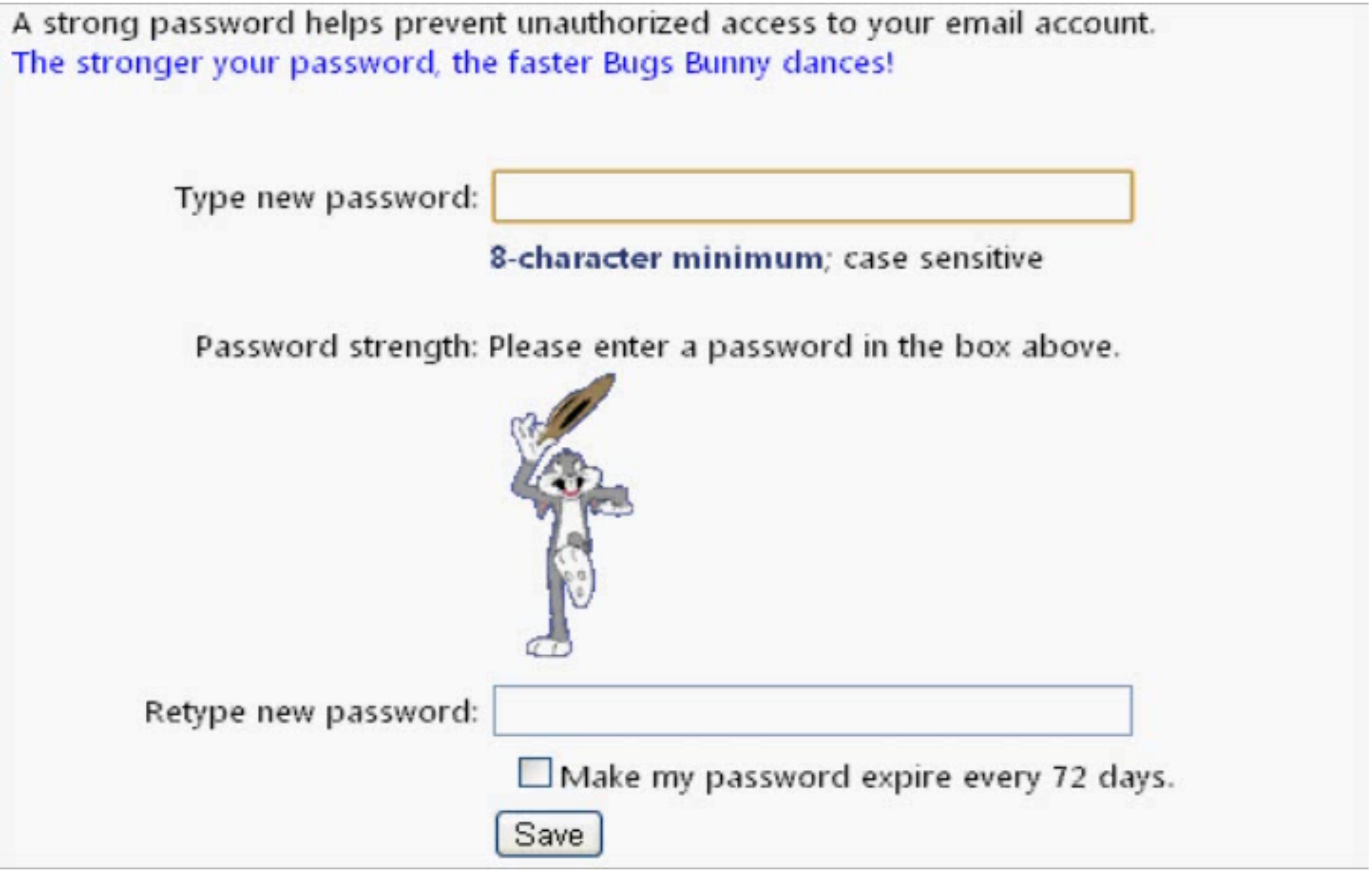
8-character minimum; case sensitive

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

Retype new password:

□ Make my password expire every 72 days.

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:

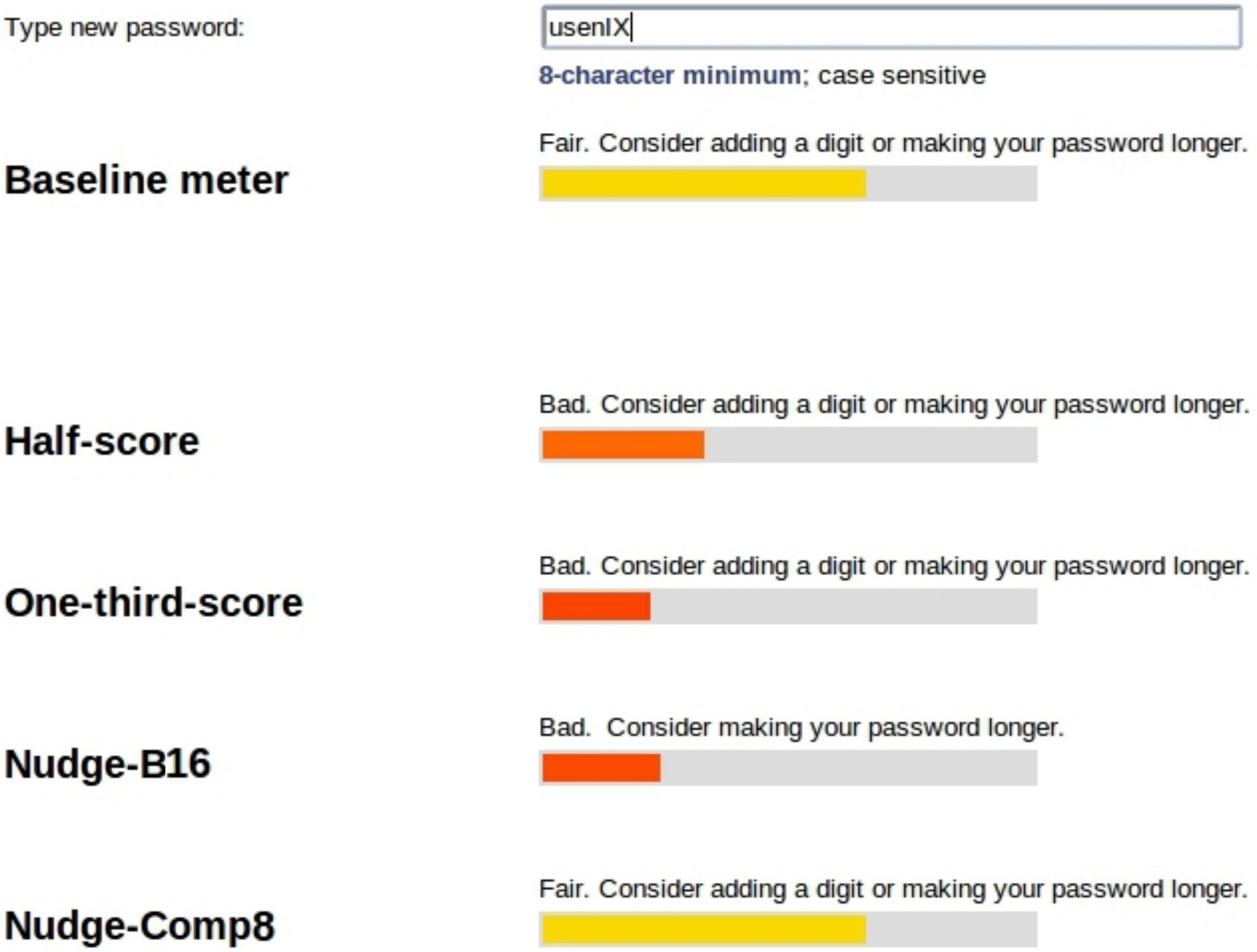
8-character minimum; case sensitive

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

Retype new password:

□ Make my password expire every 72 days.

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.

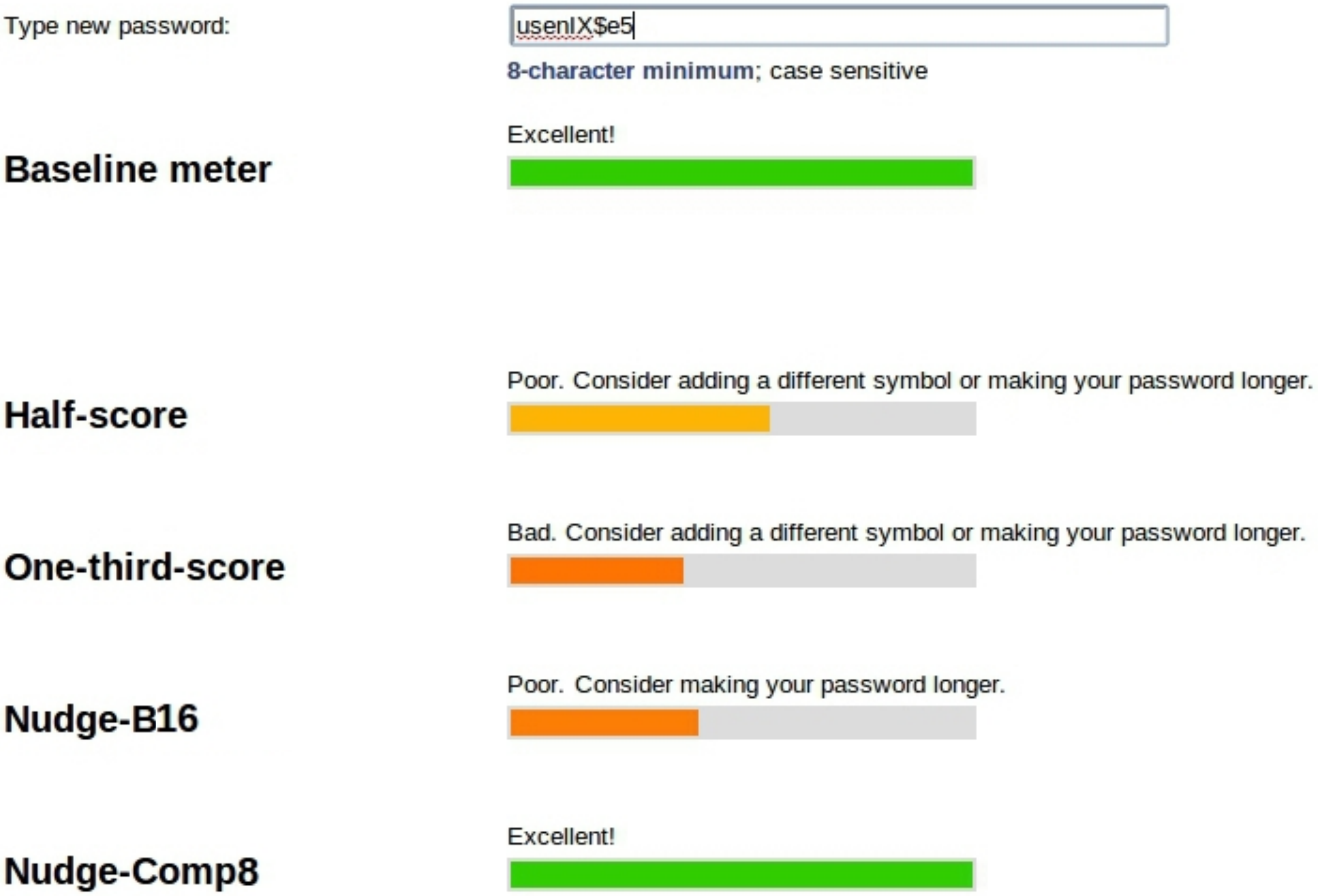
Nudge-B16

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.

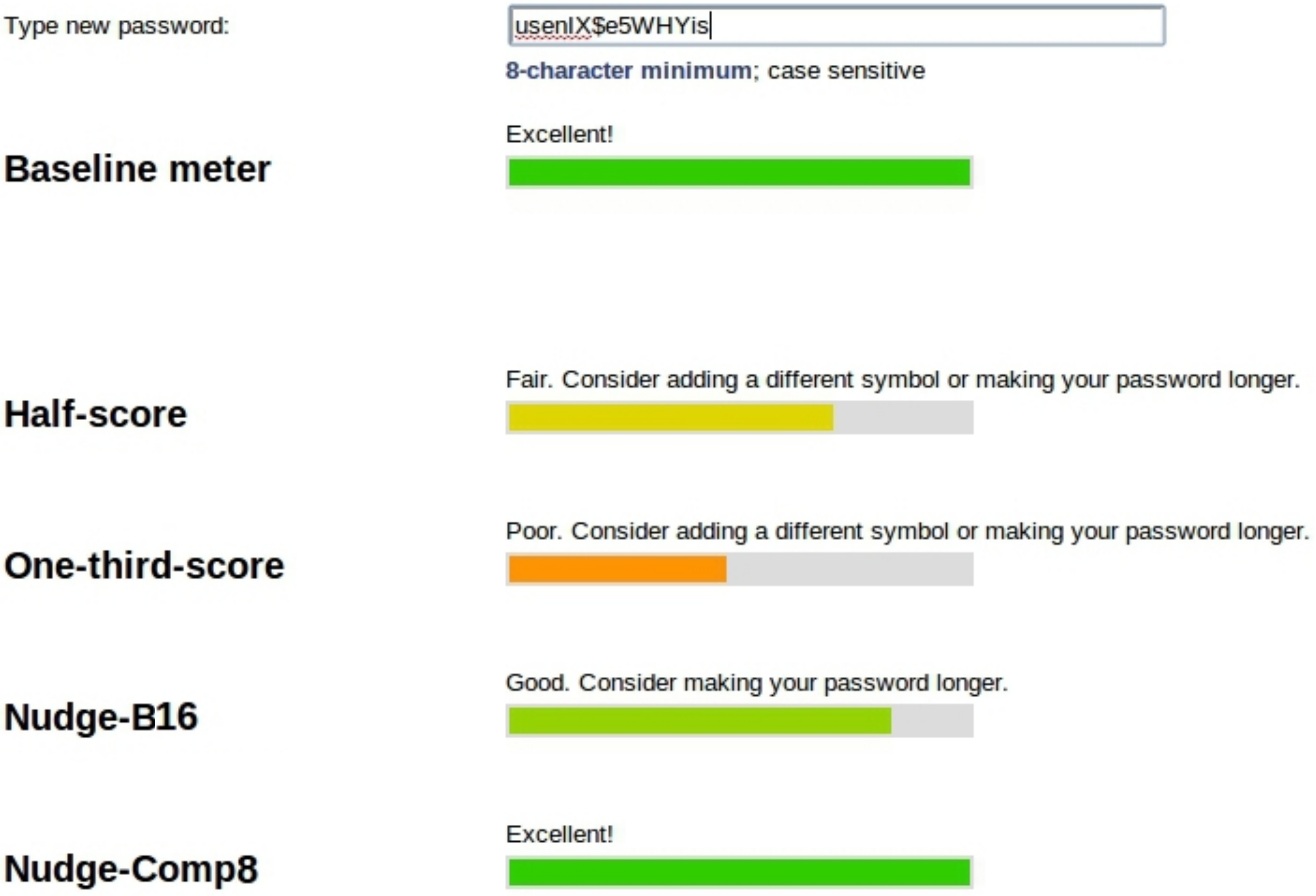
Nudge-B16

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!

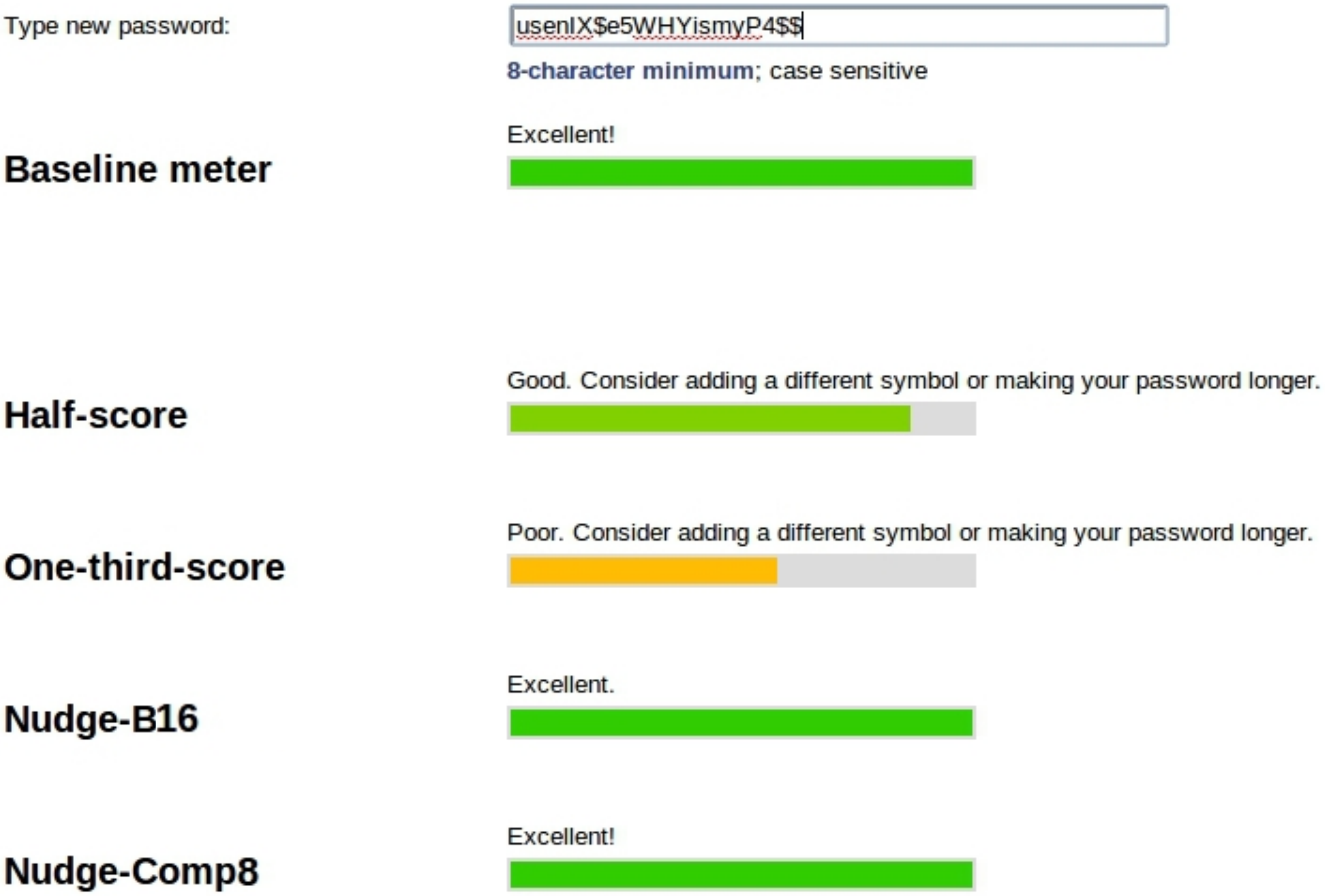
Half-score Fair. Consider adding a different symbol or making your password longer.

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.

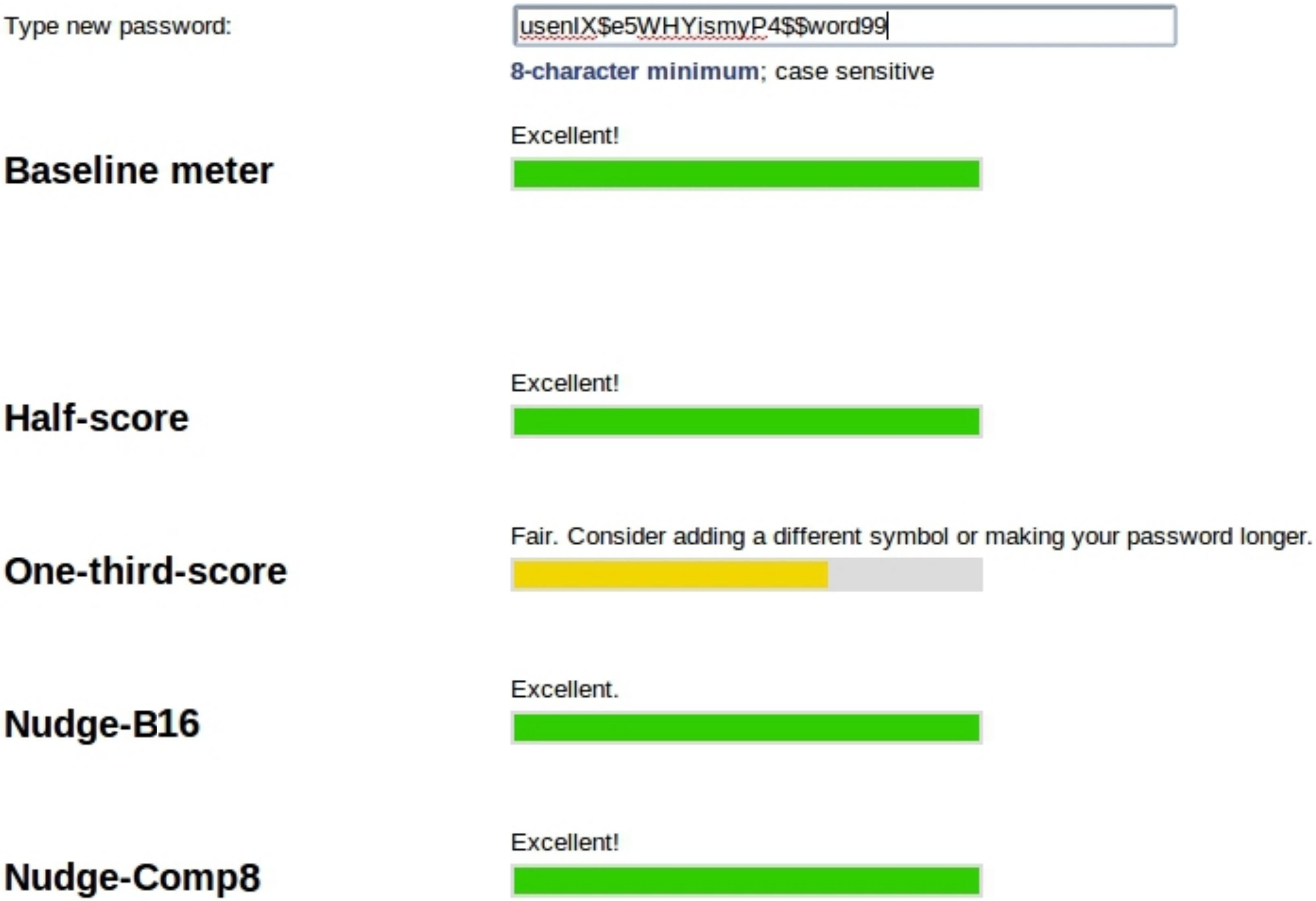
Nudge-B16

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.

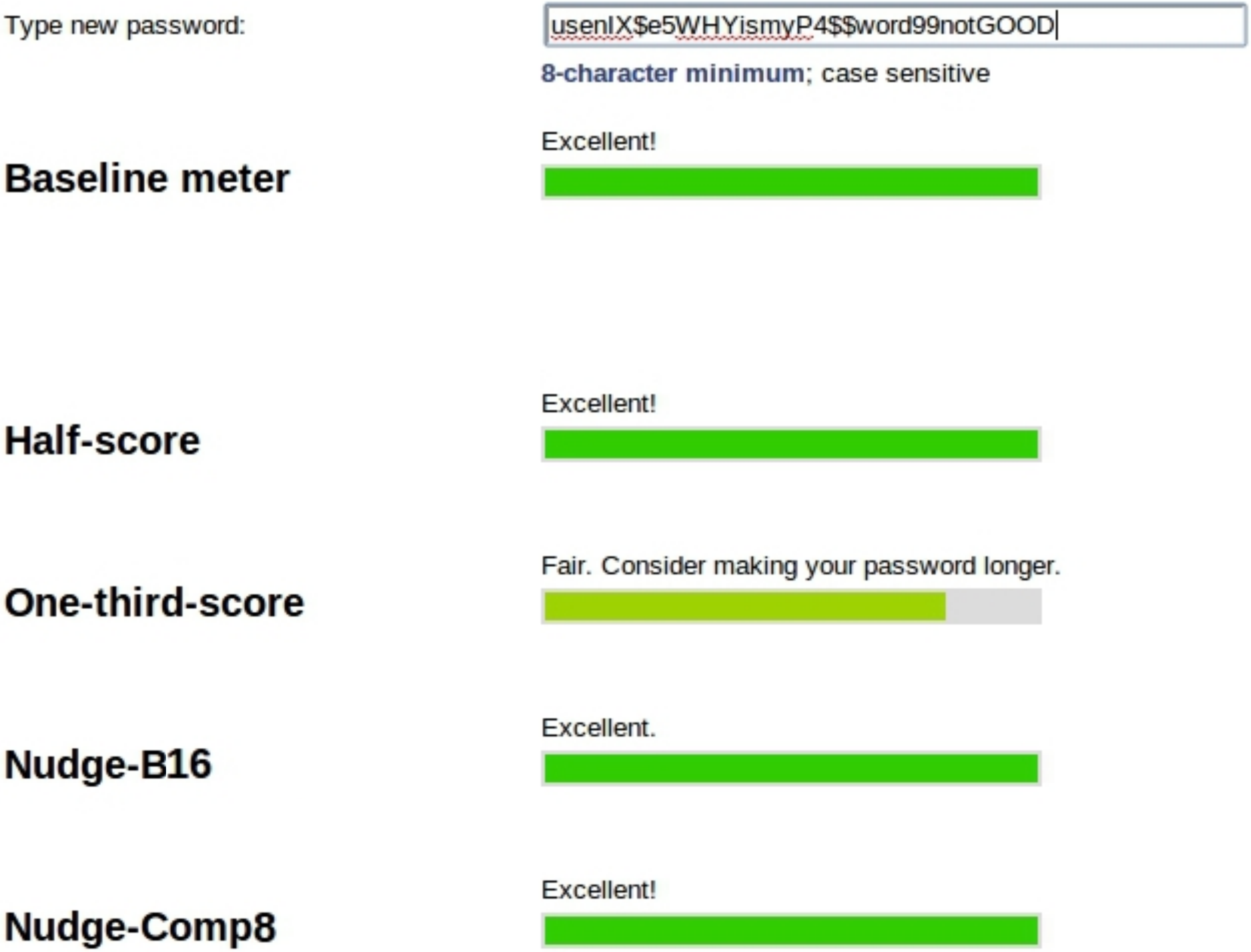
Nudge-B16

Excellent.

Nudge-Comp8

Excellent!

Conditions with Scoring Differences



Type new password: usenIX$e5WHYismyP4$$word99notGOOD

8-character minimum; case sensitive

Baseline meter

Excellent!

Half-score

Excellent!

One-third-score

Fair. Consider making your password longer.

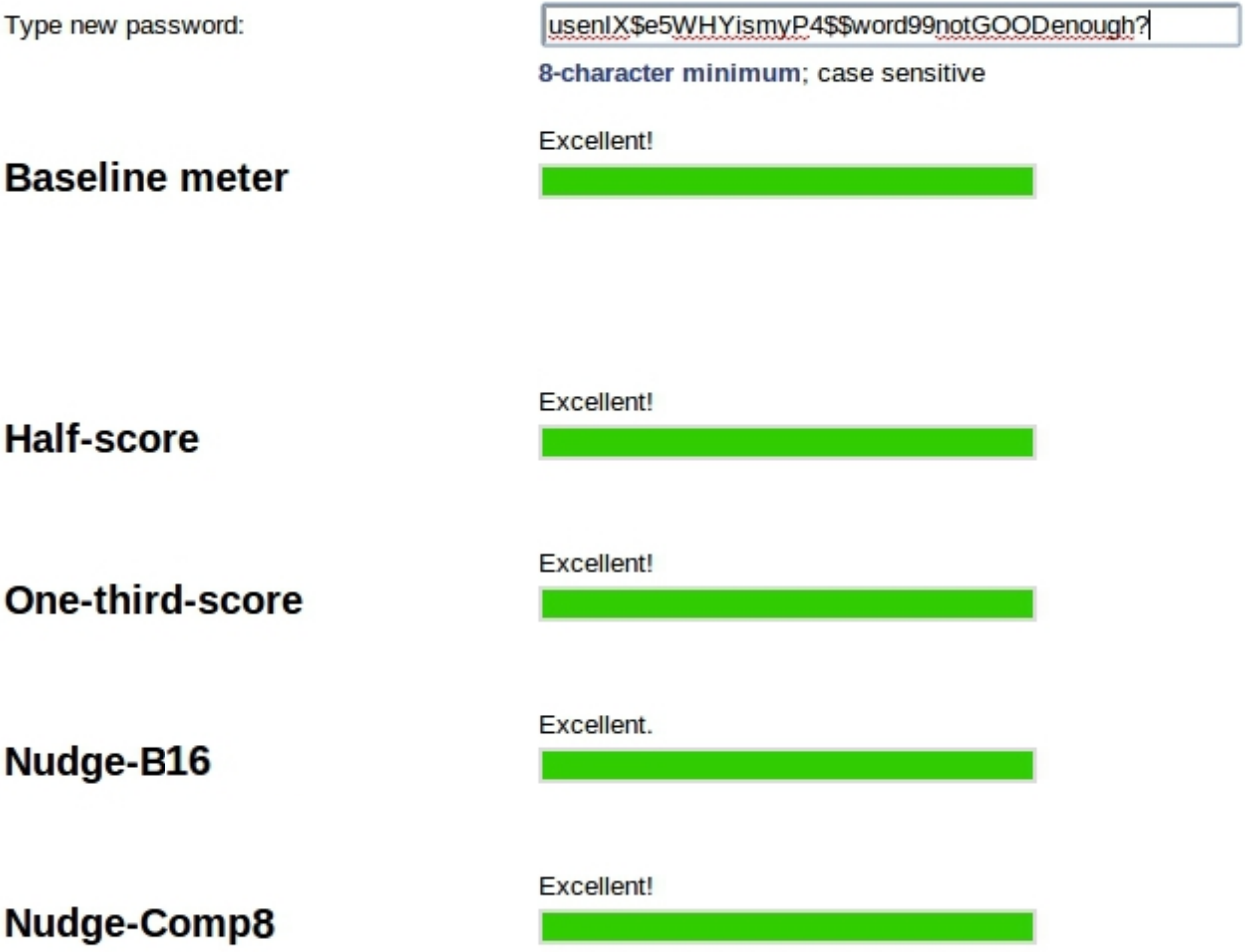
Nudge-B16

Excellent.

Nudge-Comp8

Excellent!

Conditions with Scoring Differences



Type new password: usenIX$e5WHYismyP4$$word99notGOODenough?

8-character minimum; case sensitive

Baseline meter Excellent!

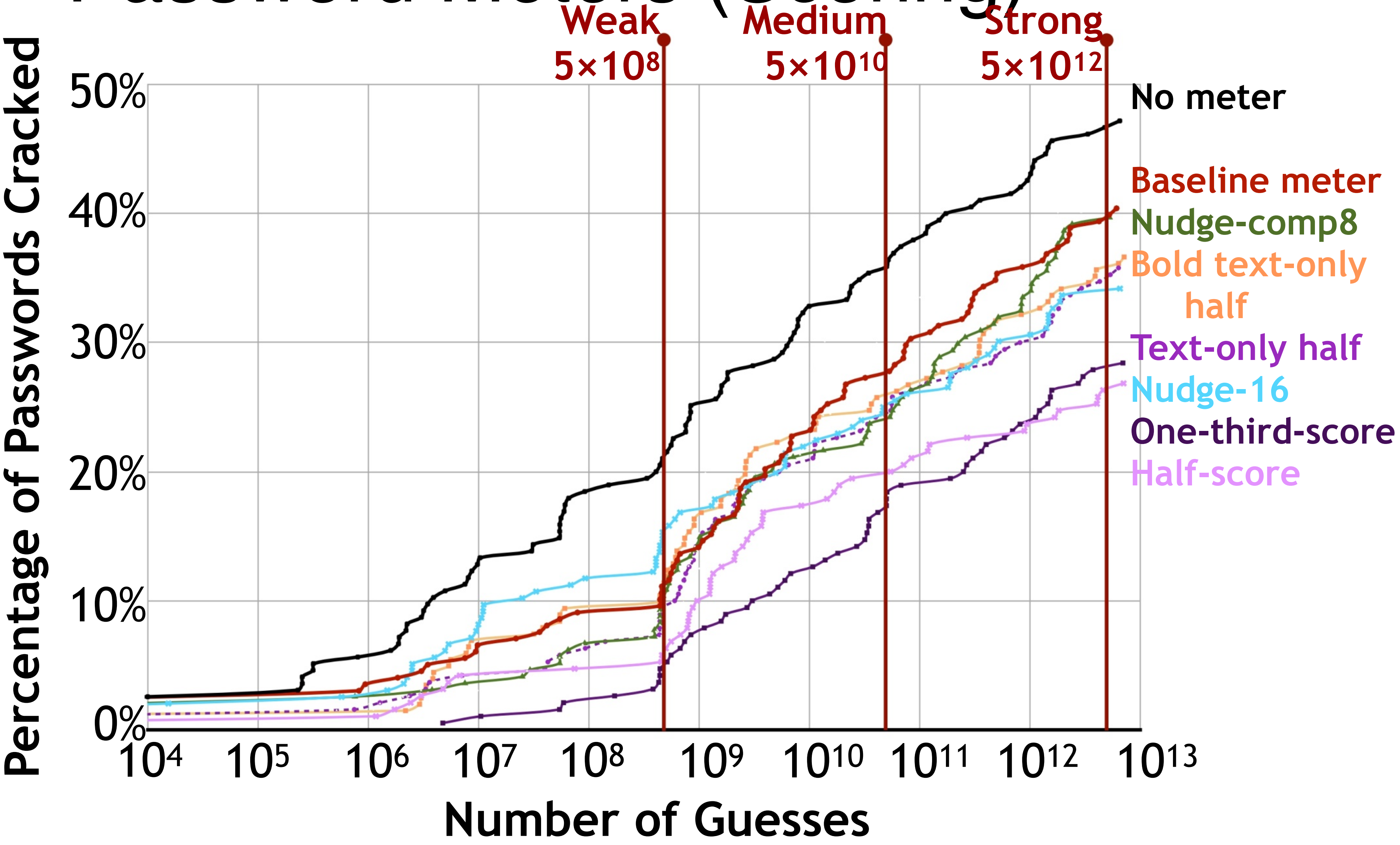
Half-score Excellent!

One-third-score Excellent!

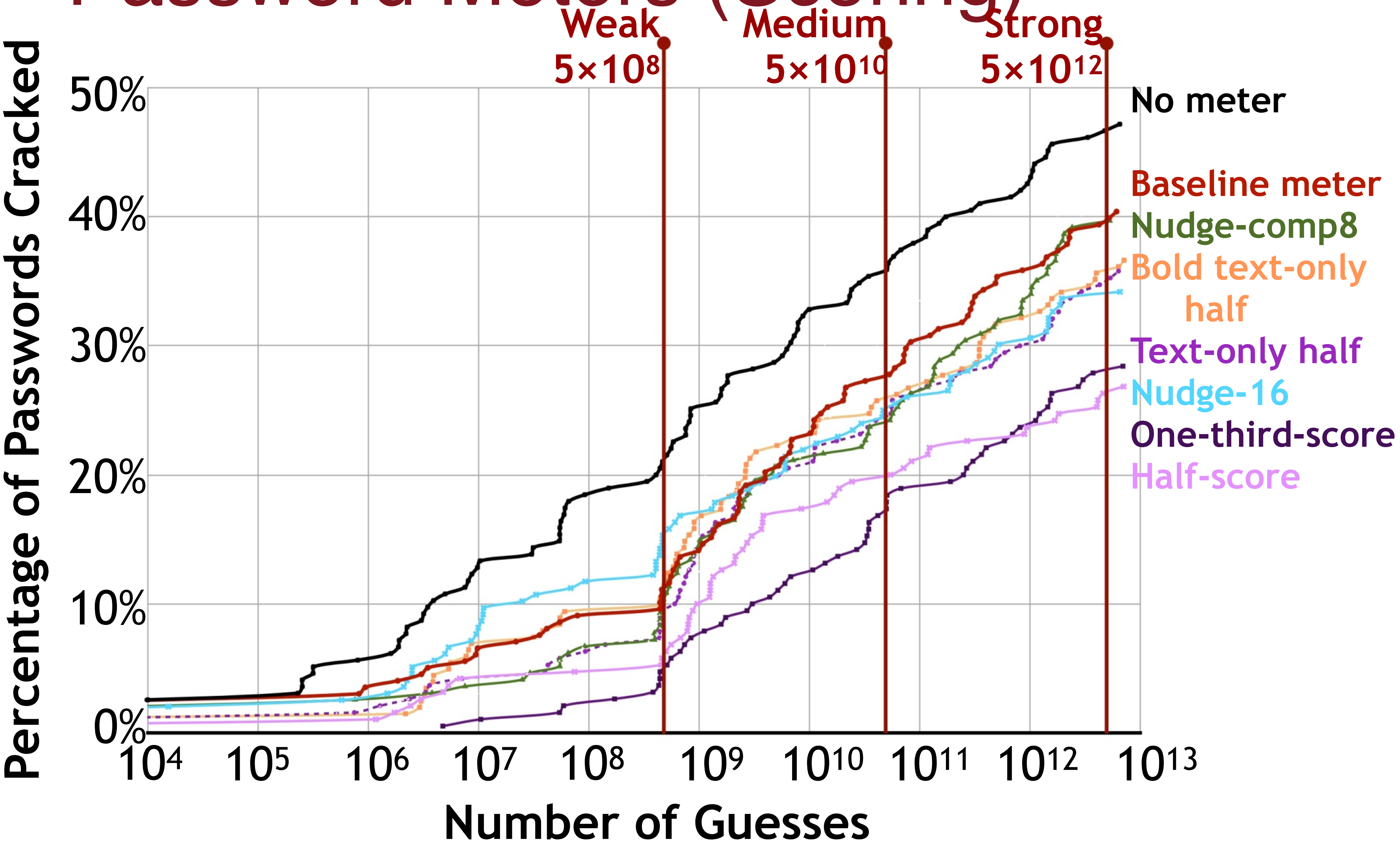
Nudge-B16 Excellent.

Nudge-Comp8 Excellent!

Password Meters (Scoring)

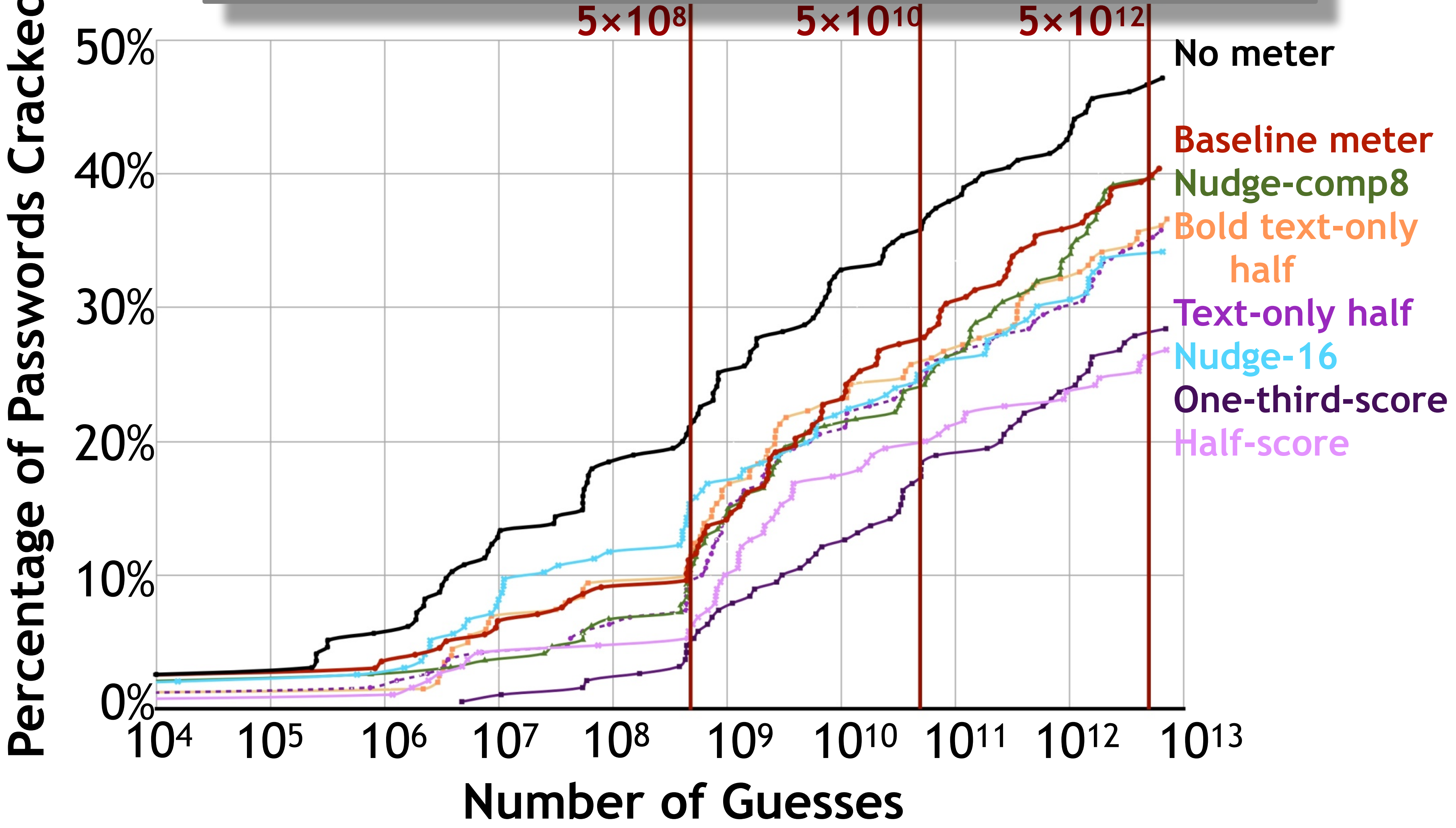


Password Meters (Scoring)



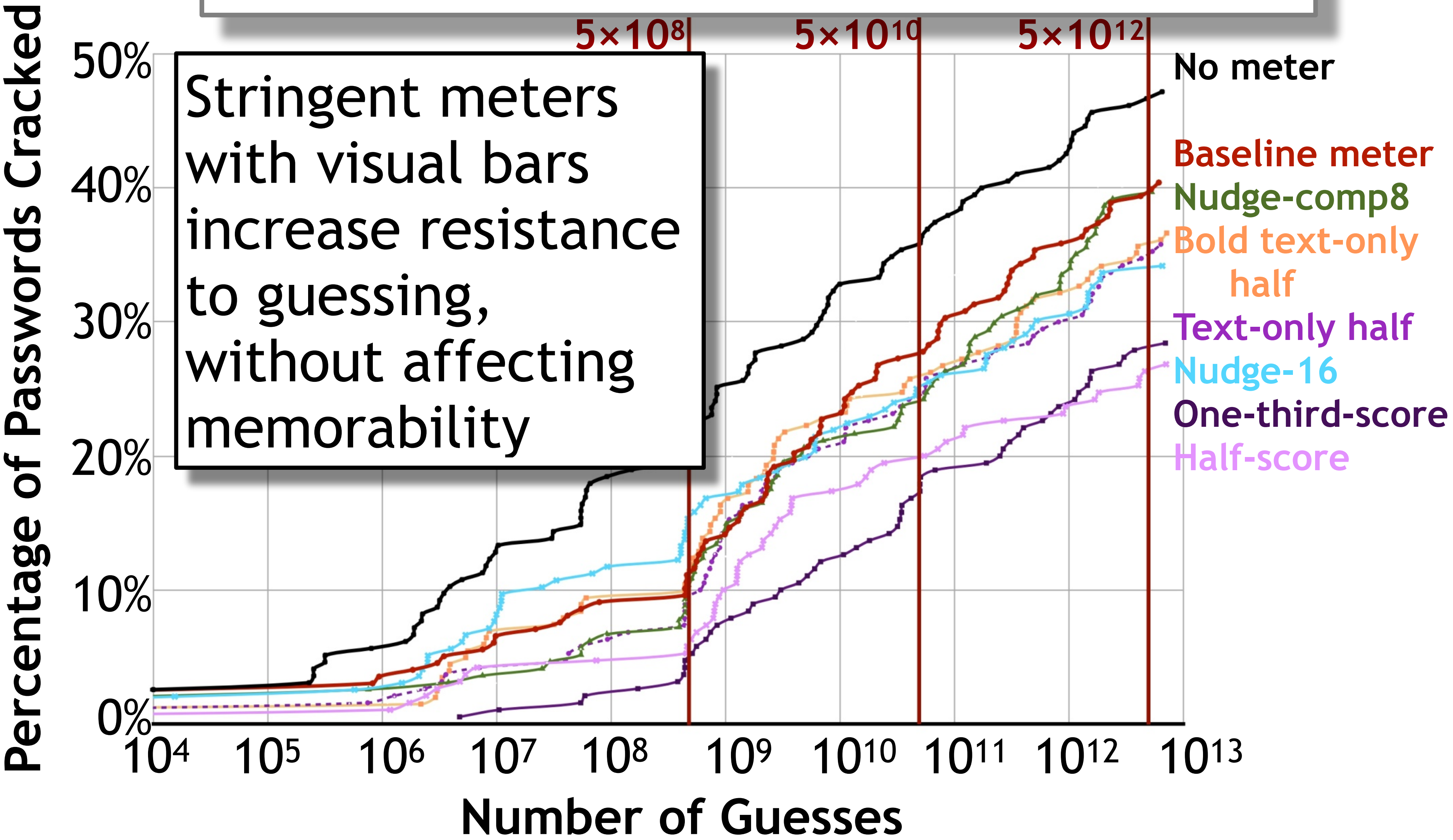
Pas

Visual changes don’t significantly increase resistance to guessing



Pas

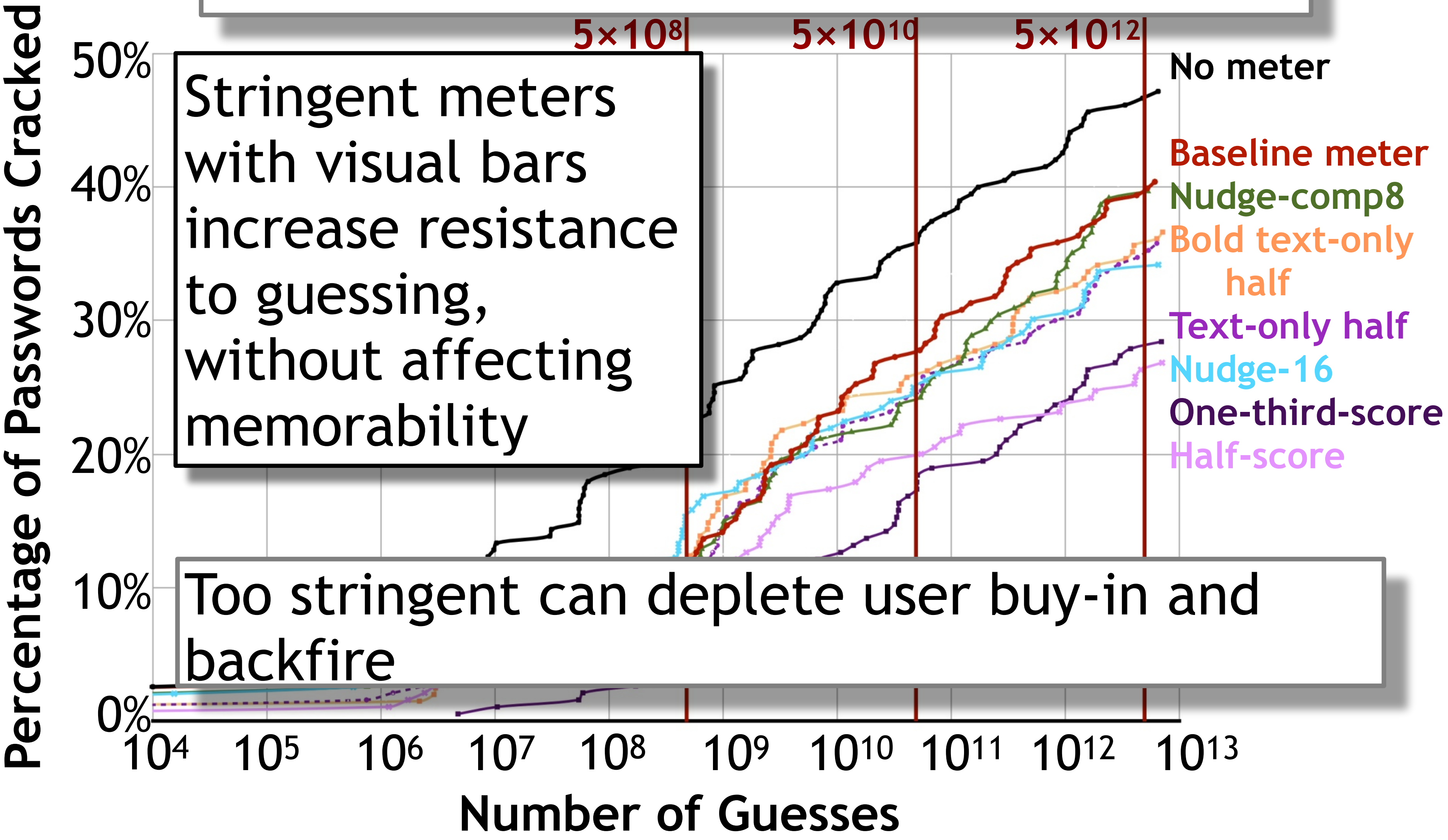
Visual changes don’t significantly increase resistance to guessing



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

Pas

Visual changes don’t significantly increase resistance to guessing



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

Too stringent can deplete user buy-in and backfire

What if the domain is not well understood?

What if the domain is not well understood?

Case Study #3: Hackers vs. Testers

http://users.umiacs.umd.edu/~dvotipka/papers/VotipkaHackerTesters2018.pdf

Vulnerability discovery

[Votipka et. al, IEEE S&P 2018]

Vulnerability discovery

Generalists

Experts

Research Questions

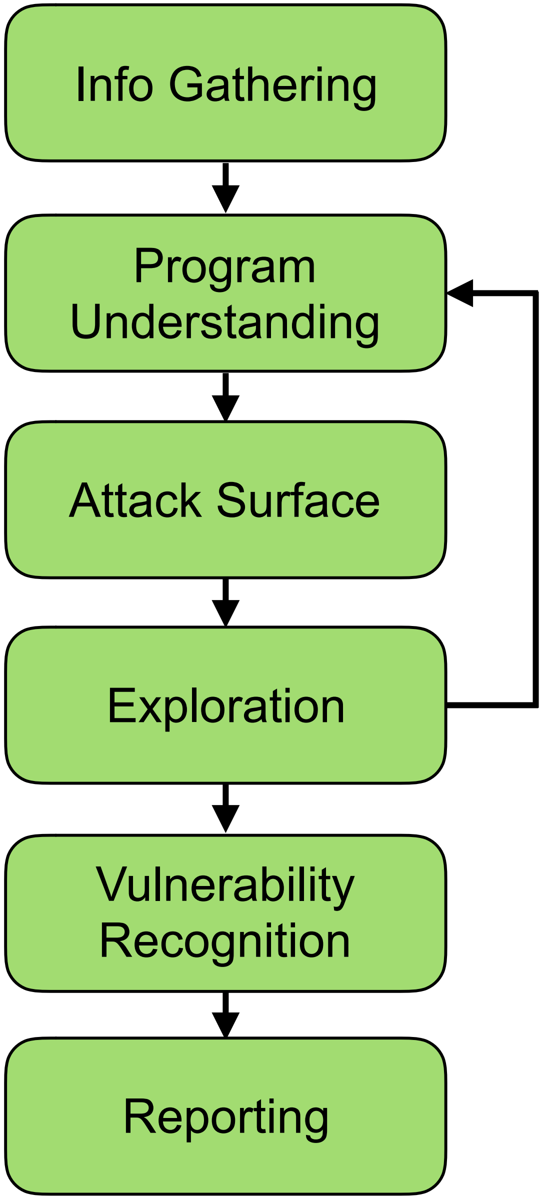
1. How do testers and hackers search for vulnerabilities?
2. What are the differences between testers and hackers?

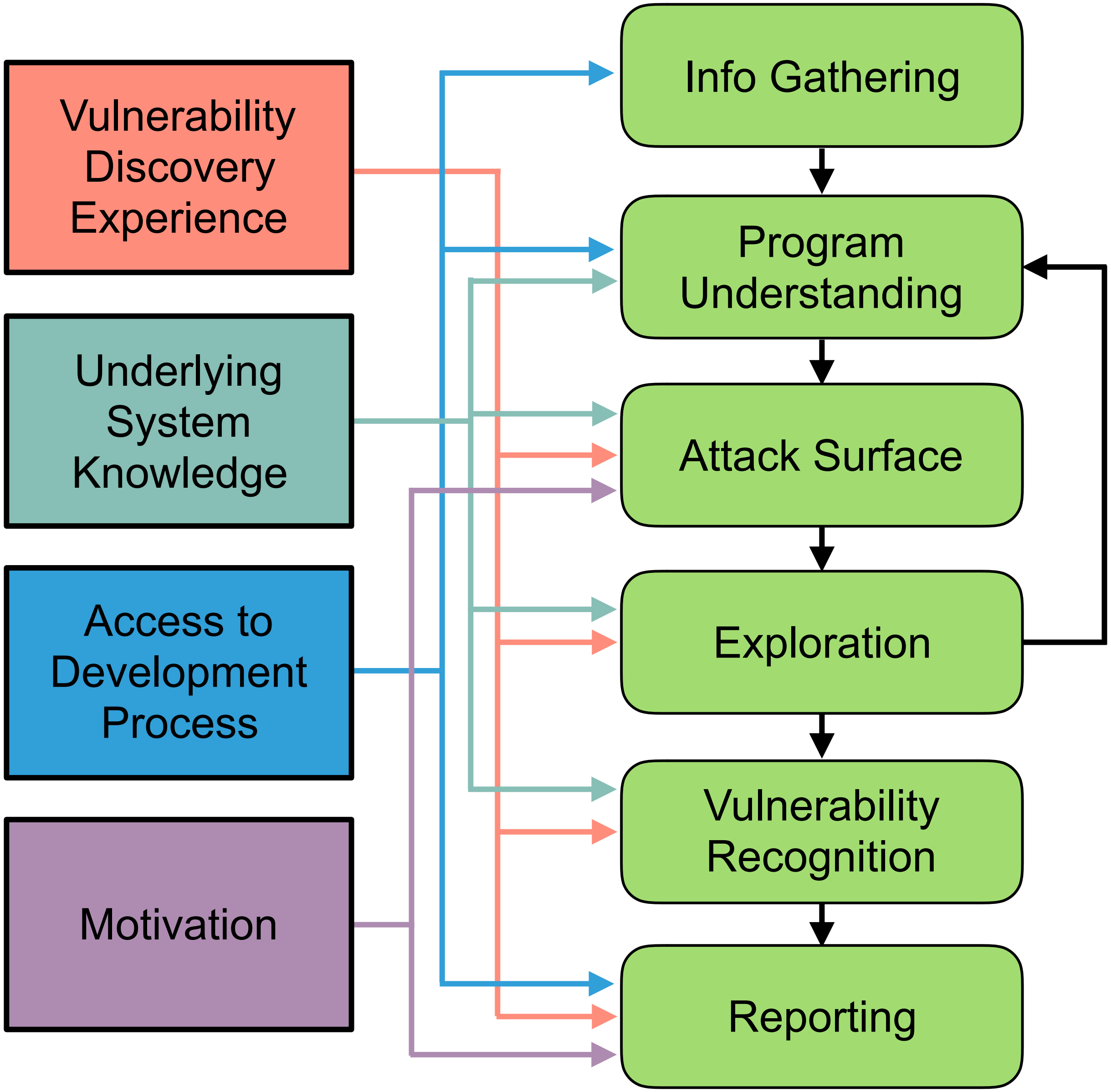
Research Questions

1. How do testers and hackers search for vulnerabilities?
2. What are the differences between testers and hackers?

Interview study:

- Task Analysis
- Tools, Skills, and Communities


Info Gathering
Program Understanding
Attack Surface
Exploration
Vulnerability Recognition
Reporting



Vulnerability Discovery Experience

Underlying System Knowledge

Access to Development Process

Motivation

Info Gathering

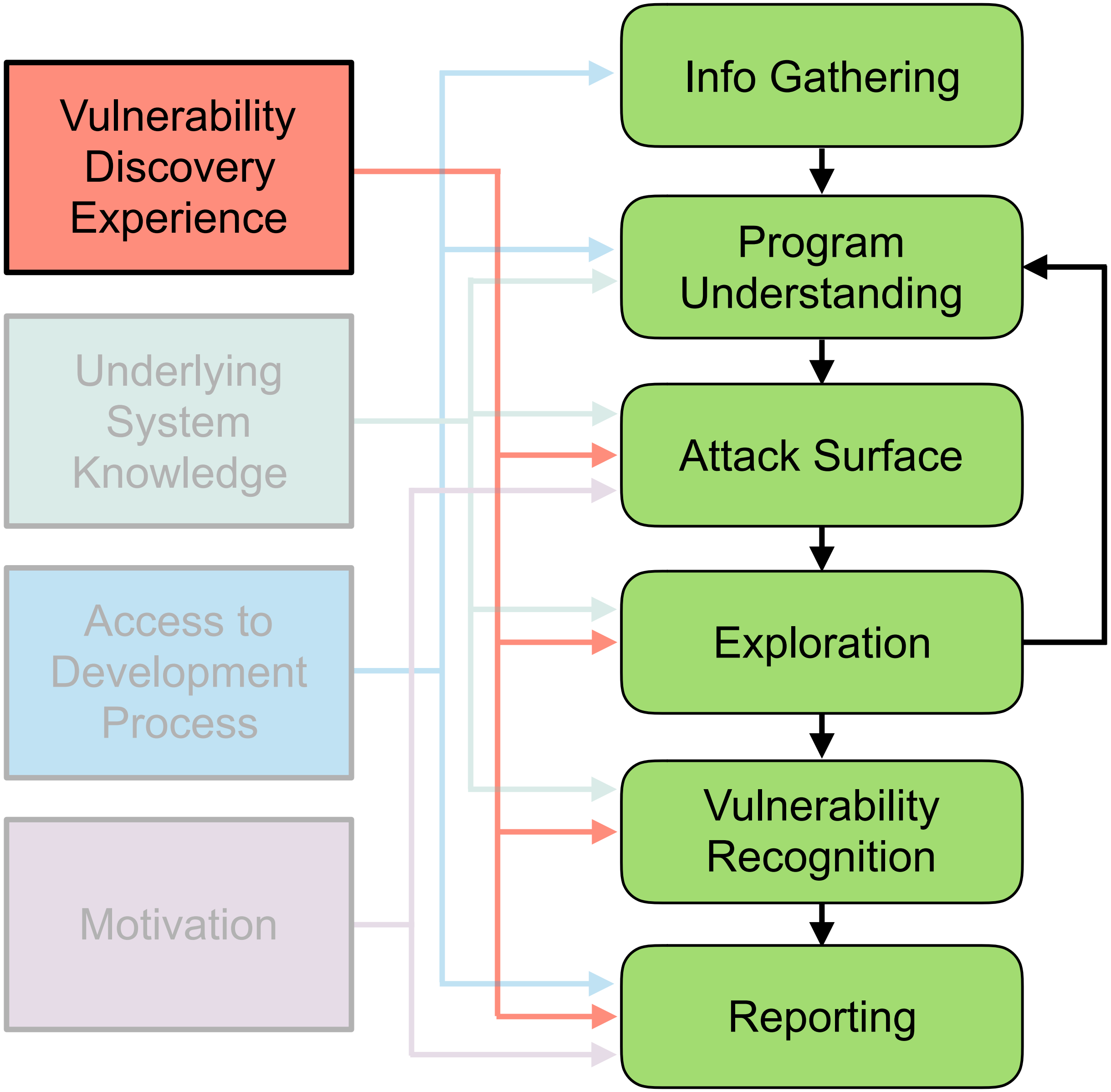
Program Understanding

Attack Surface

Exploration

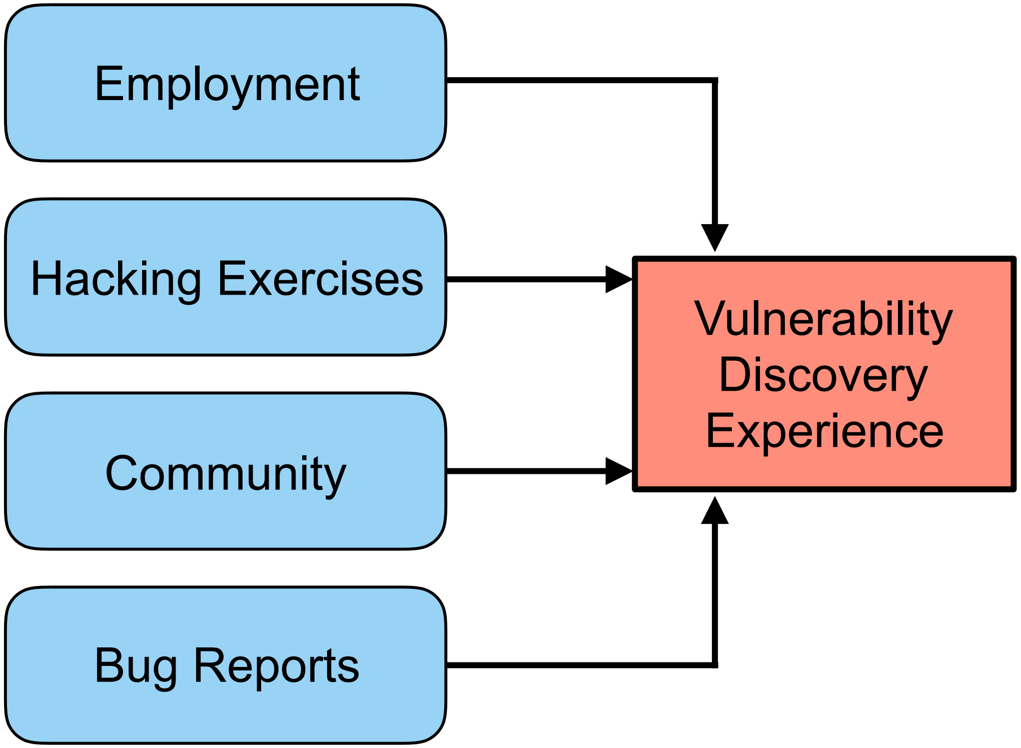
Vulnerability Recognition

Reporting



Vulnerability Discovery Experience
Underlying System Knowledge
Access to Development Process
Motivation
Info Gathering
Program Understanding
Attack Surface
Exploration
Vulnerability Recognition
Reporting

Amount of experience



Employment

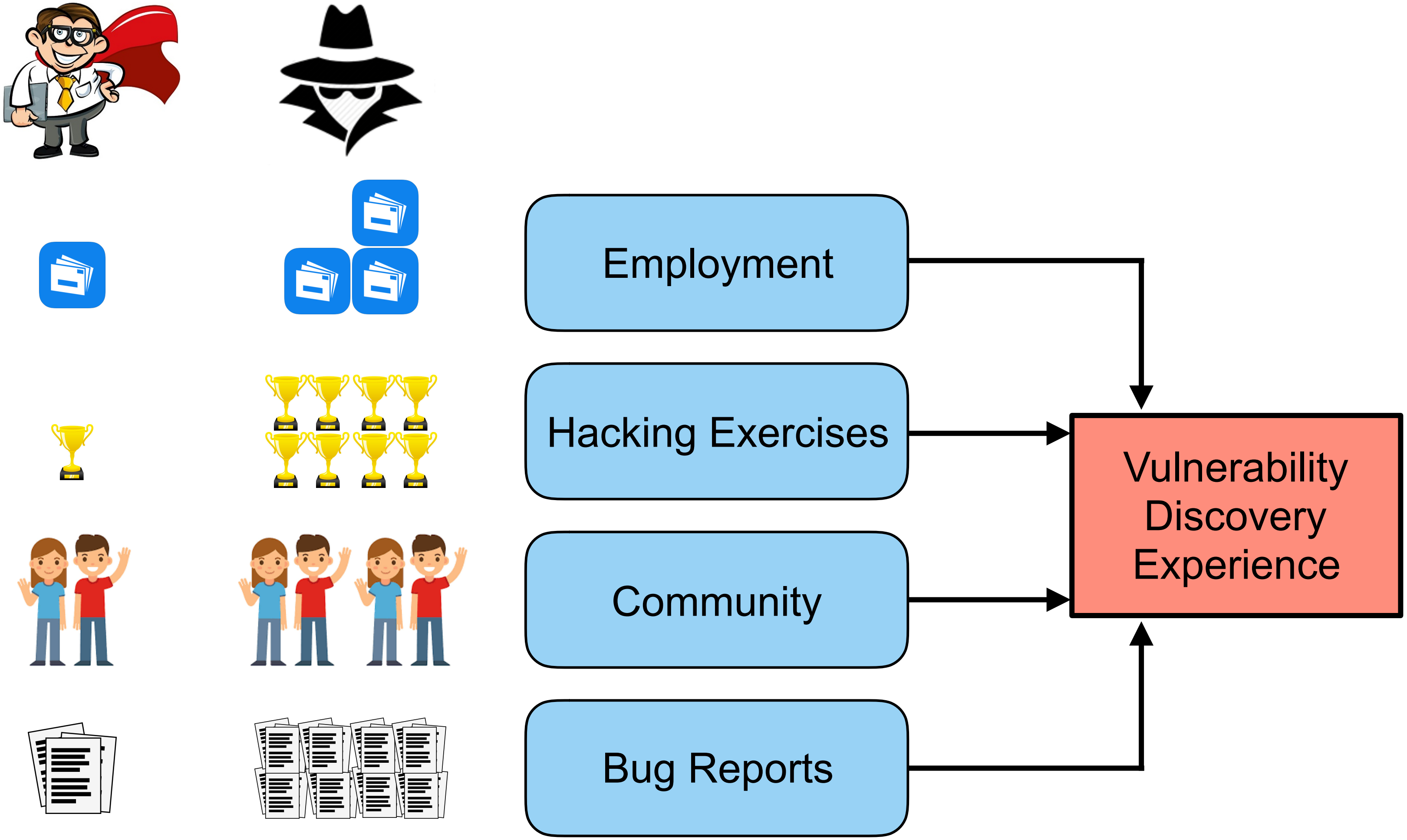
Hacking Exercises

Community

Bug Reports

Vulnerability Discovery Experience

Amount of experience



Employment

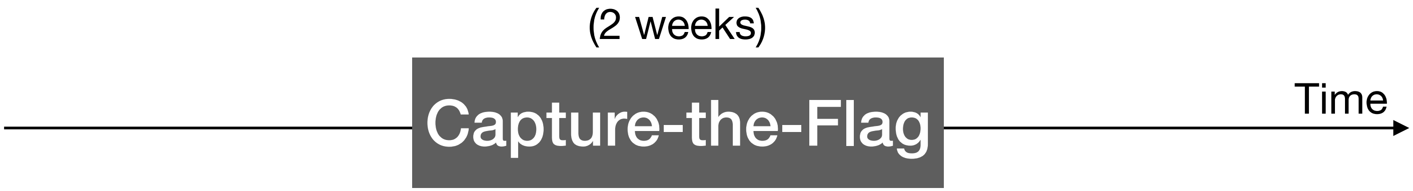
Hacking Exercises

Community

Bug Reports

Vulnerability Discovery Experience

Hacking exercises



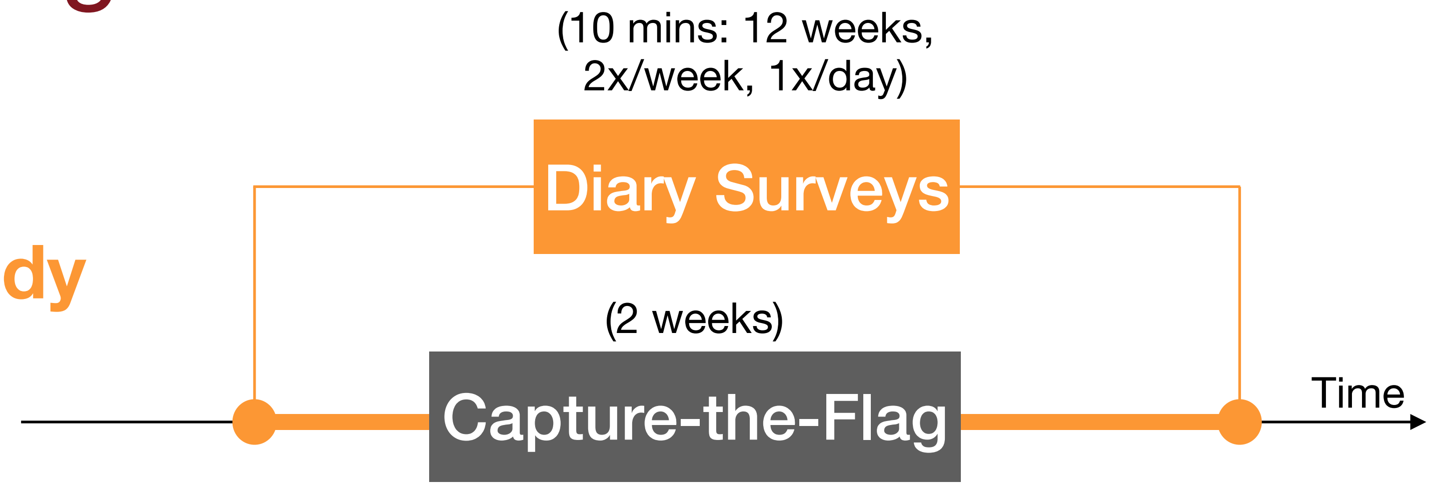
(2 weeks)

Capture-the-Flag

Time

Hacking exercises

Diary Study

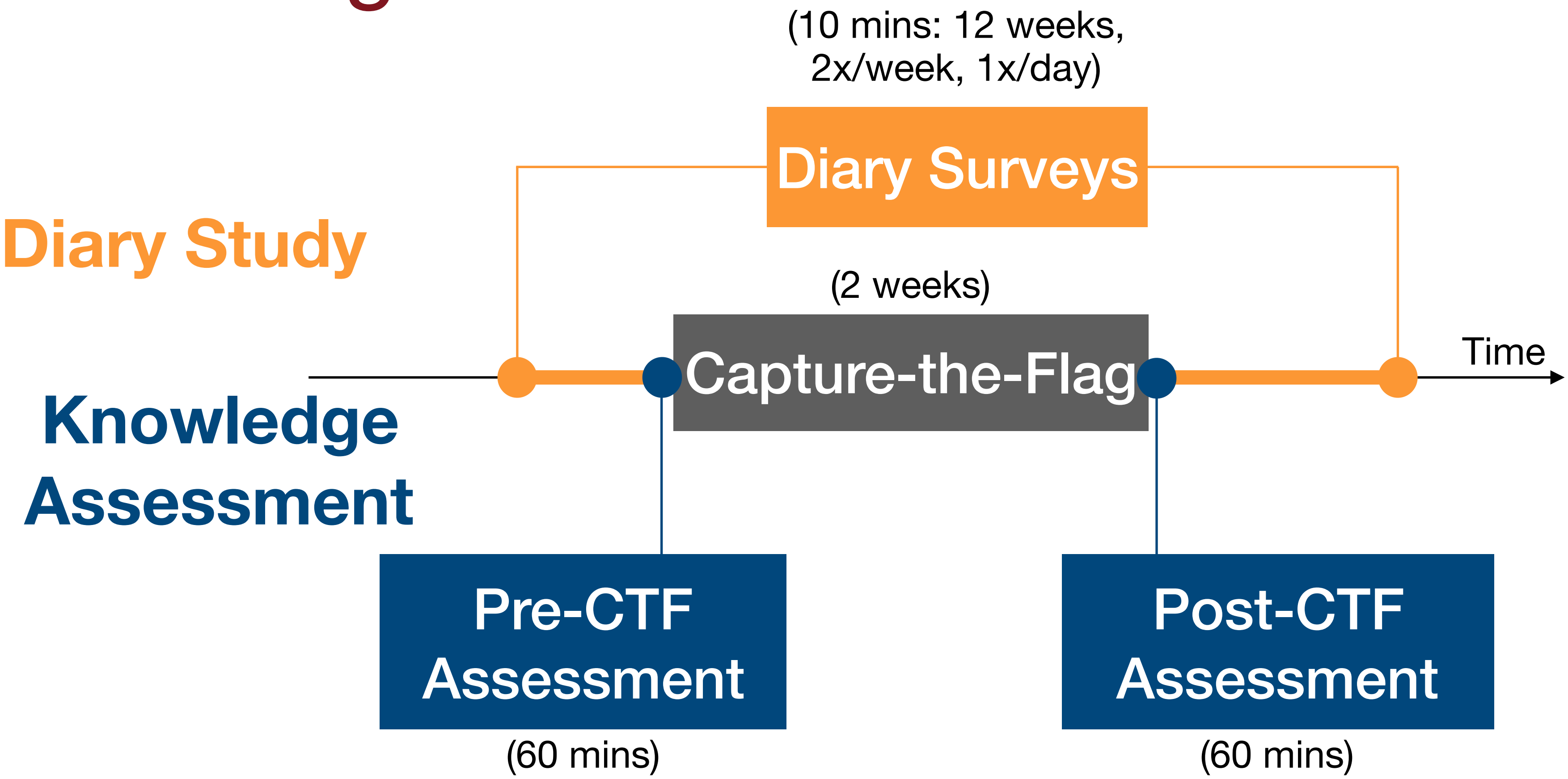

(10 mins: 12 weeks, 2x/week, 1x/day)

Diary Surveys

(2 weeks)

Capture-the-Flag

Hacking exercises



Diary Study

(10 mins: 12 weeks, 2x/week, 1x/day)

Diary Surveys

(2 weeks)

Capture-the-Flag

Time

Knowledge Assessment

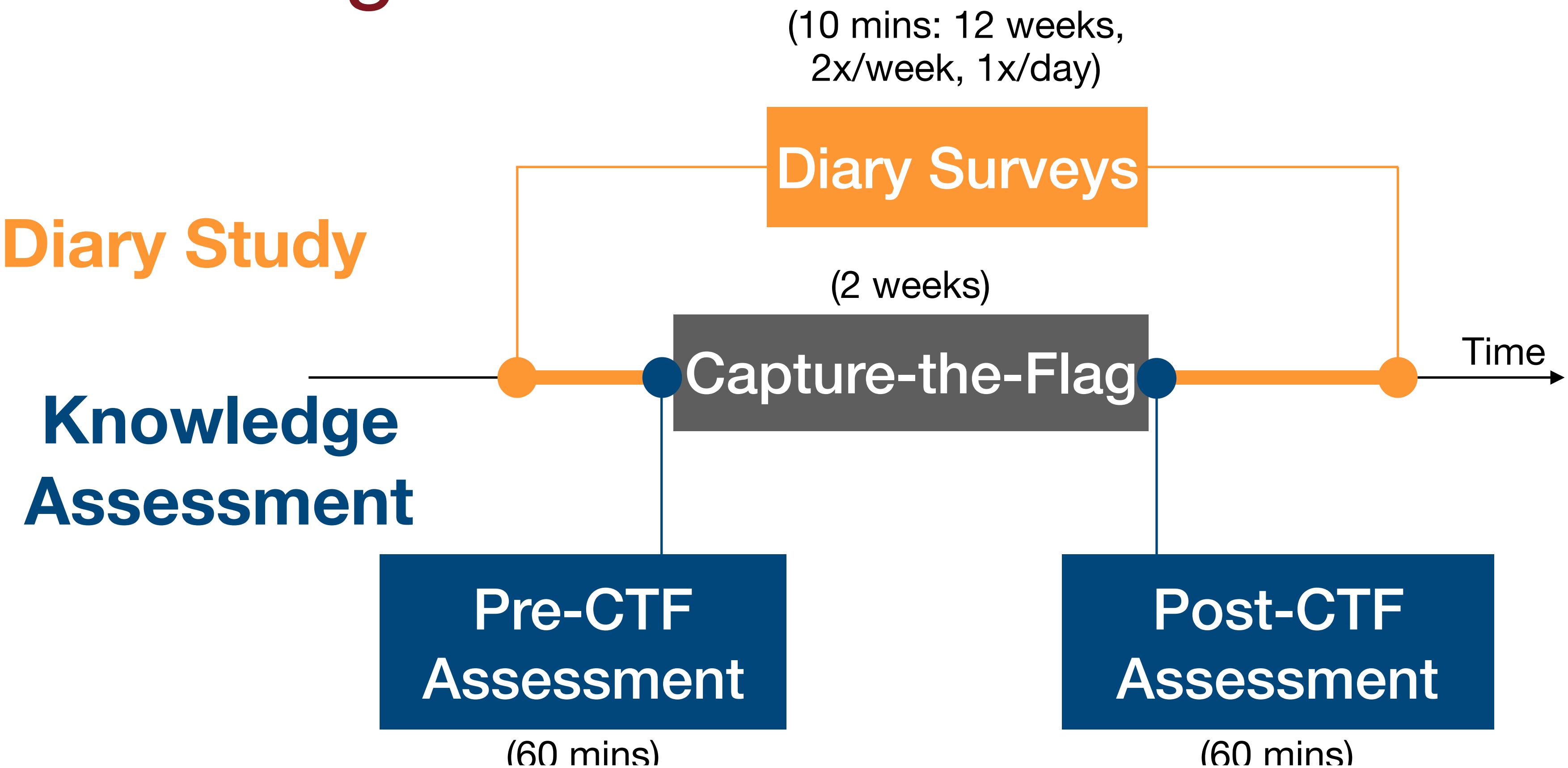
Pre-CTF Assessment

(60 mins)

Post-CTF Assessment

(60 mins)

Hacking exercises



(10 mins: 12 weeks,
2x/week, 1x/day)

Diary Surveys

Diary Study

(2 weeks)

Capture-the-Flag

Time

Knowledge Assessment

Pre-CTF Assessment

(60 mins)

Post-CTF Assessment

(60 mins)

Dropbox

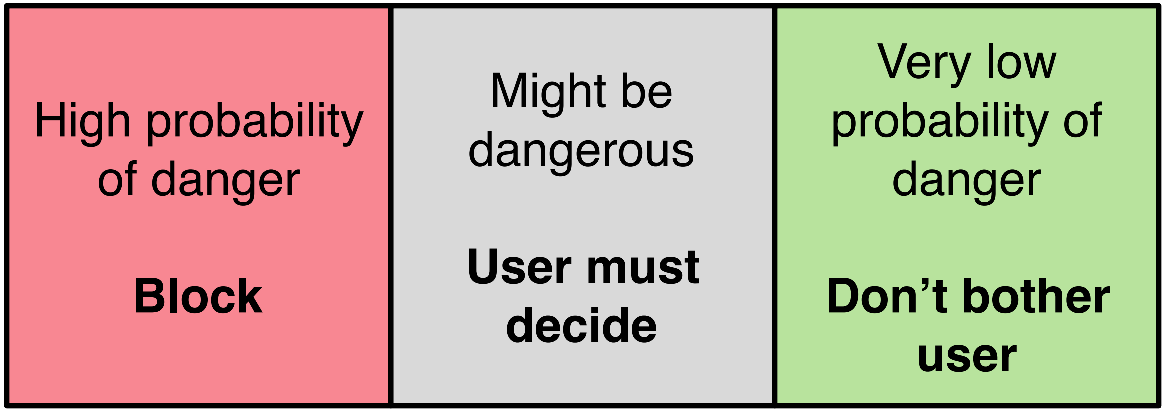
https://www.umiacs.umd.edu/~dvotipka/papers/VotipkaDropboxCTF2018.pdf

Making things better

Use psychology in your favor

- Limit memory requirements
- Grab attention when you need it
- Make critical information stand out / avoid habituation
- Minimize effort:
    - To get users to take action, make it easy
    - To get users to avoid danger, make it difficult

Limit the user’s cognitive load



High probability of danger

Block

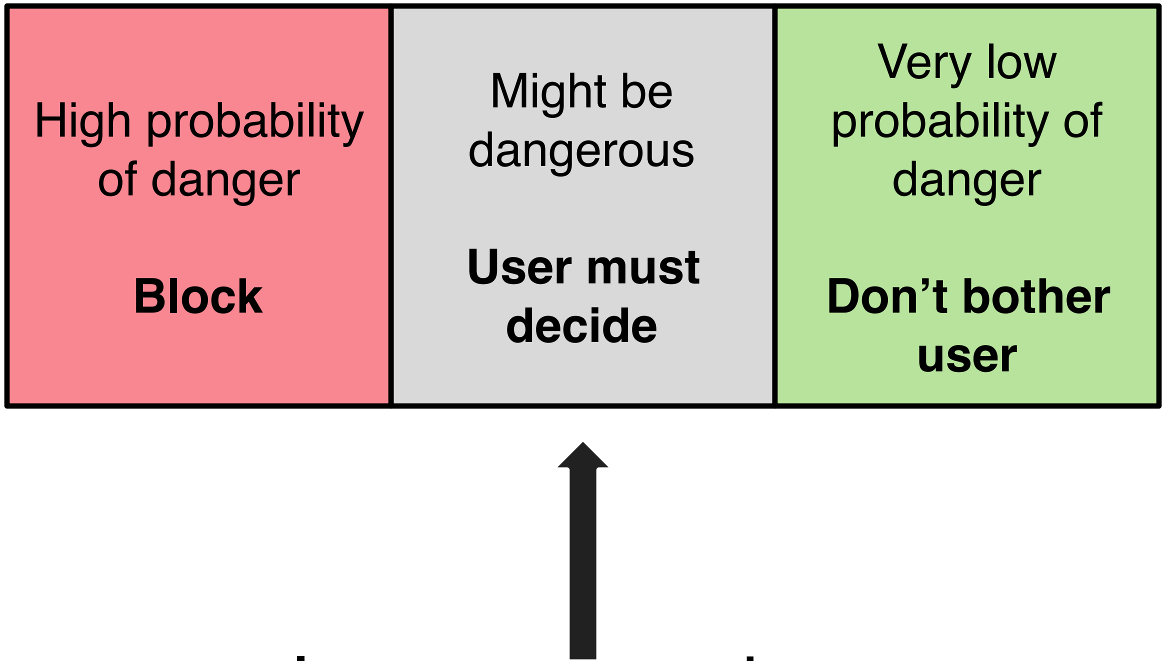
Might be dangerous

User must decide

Very low probability of danger

Don’t bother user

Limit the user's cognitive load



High probability of danger

Block

Might be dangerous

User must decide

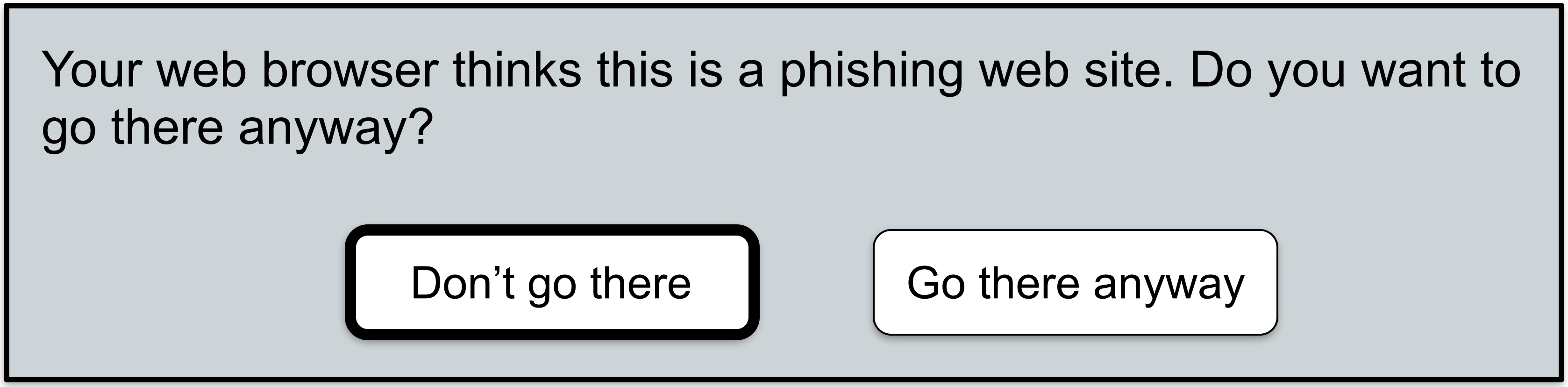
Very low probability of danger

Don't bother user

Improve warnings

Help user decide by asking a question user is qualified to answer

Bad question



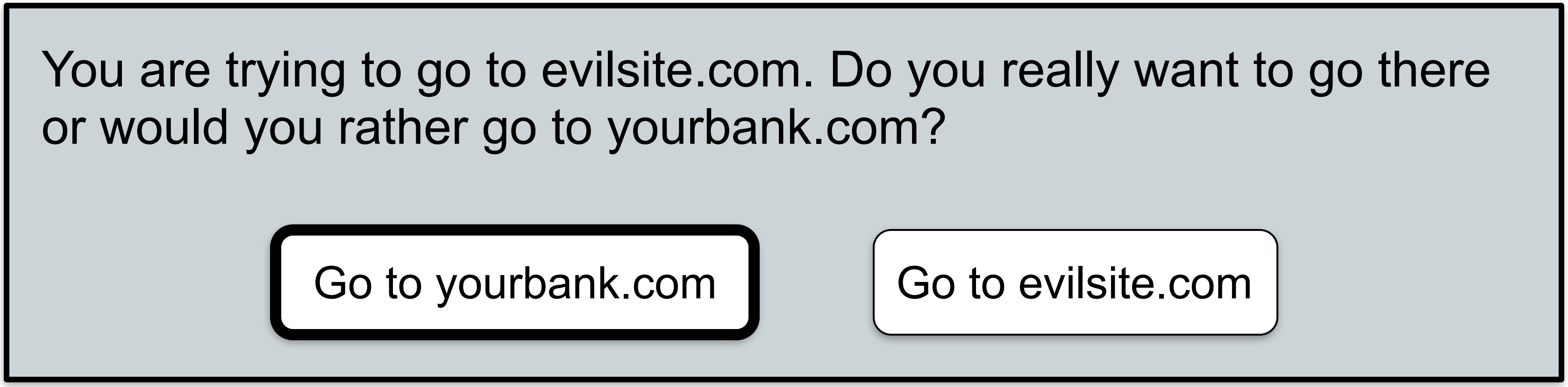
Your web browser thinks this is a phishing web site. Do you want to go there anyway?

I don’t know what a phishing site is.

I really want to go to this site.

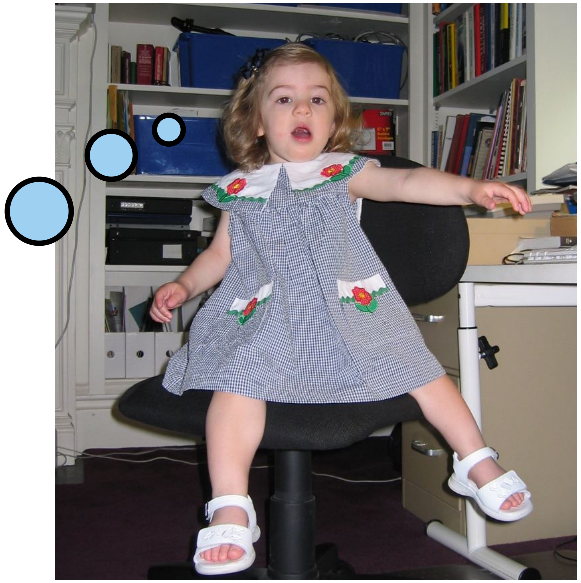
Of course I will go there anyway!

Better question



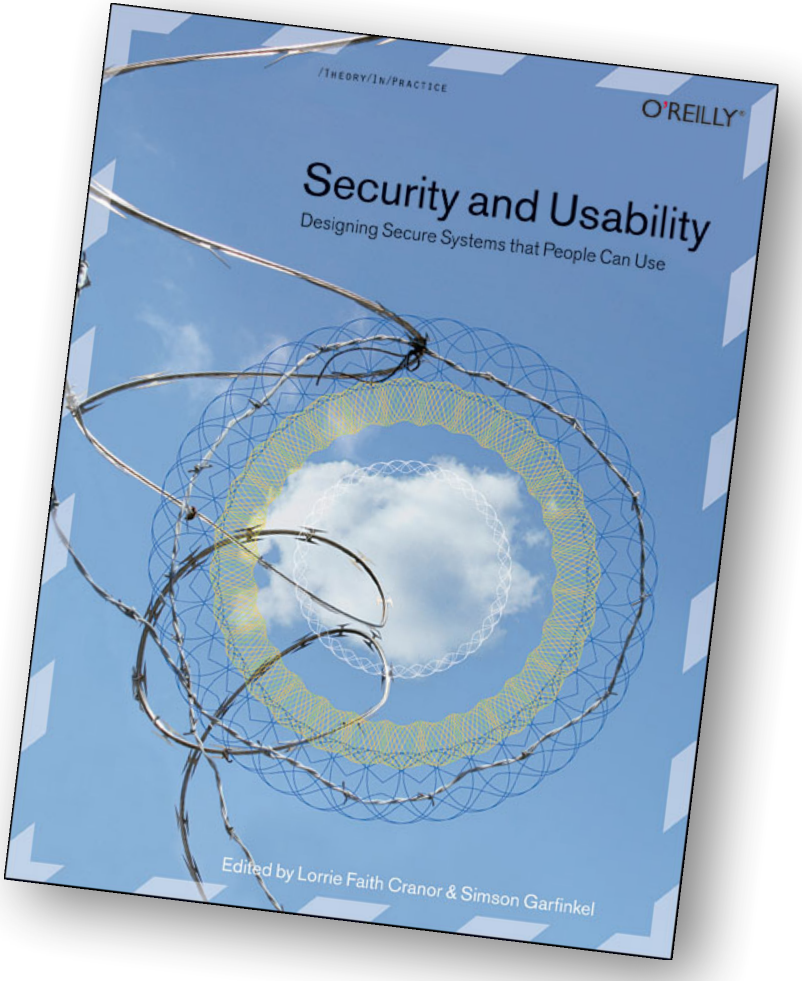
You are trying to go to evilsite.com. Do you really want to go there or would you rather go to yourbank.com?

Of course I want to go to yourbank.com!



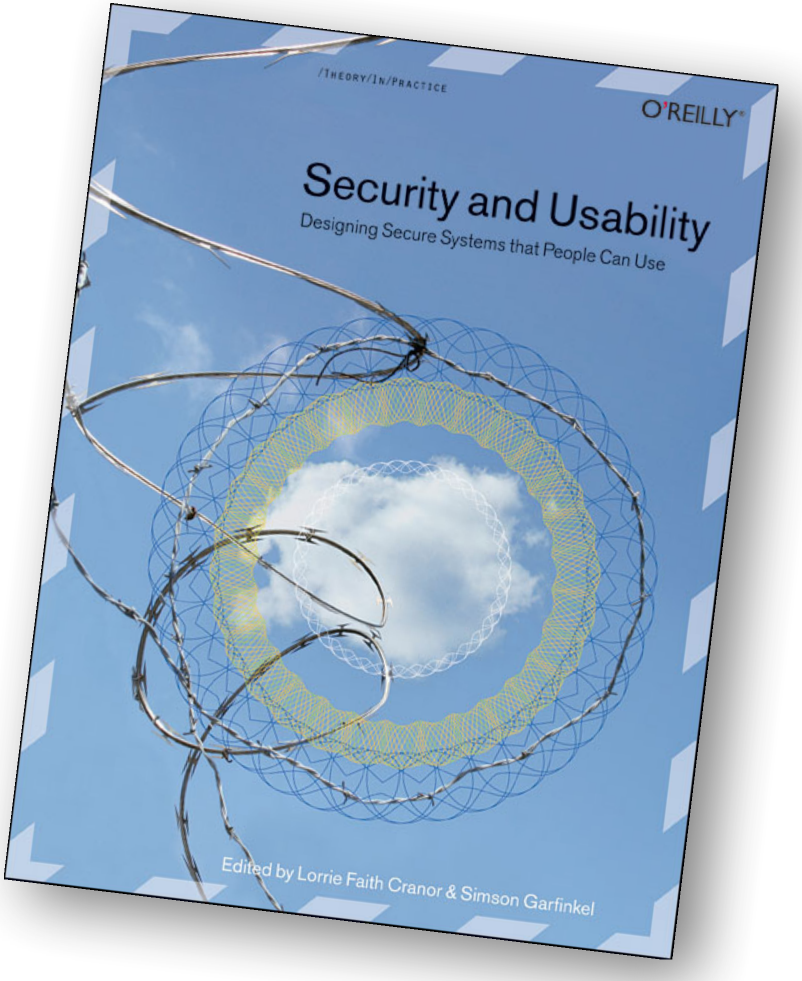
Hierarchy of solutions

- 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

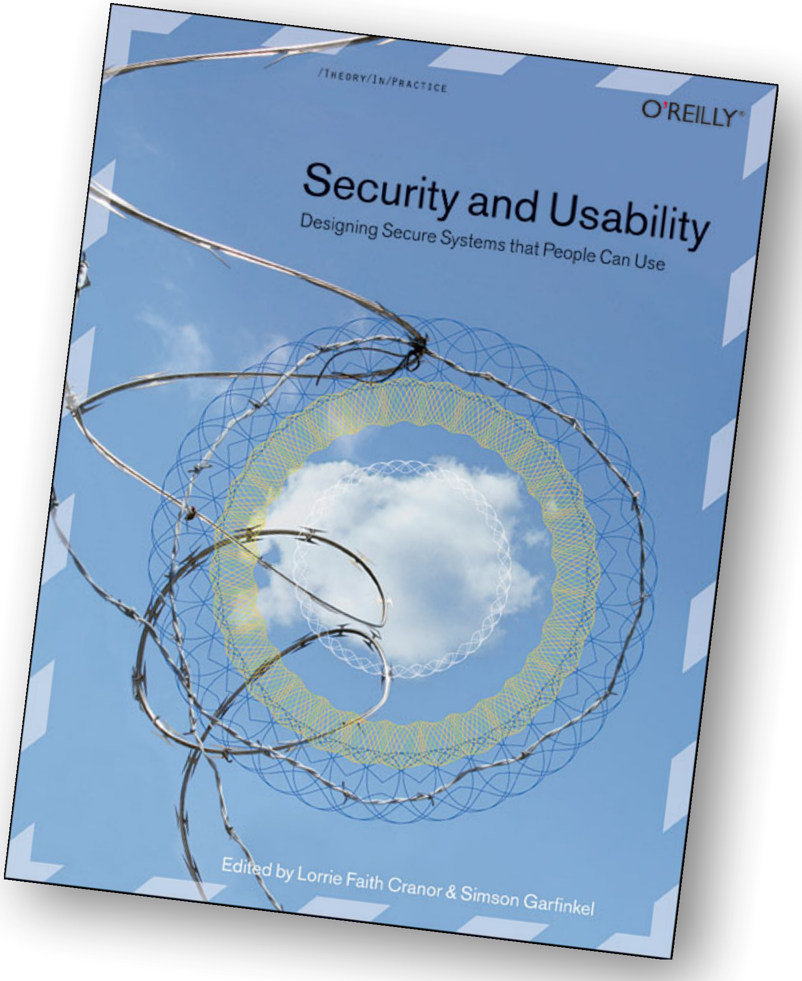
Want to learn more?

Want to learn more?



/Theory/In/Practice
O'REILLY
Security and Usability
Designing Secure Systems that People Can Use
Edited by Lorrie Faith Cranor & Simson Garfinkel

Want to learn more?



/THEORY/IN/PRACTICE

O'REILLY®

Security and Usability

Designing Secure Systems that People Can Use

Edited by Lorrie Faith Cranor & Simson Garfinkel

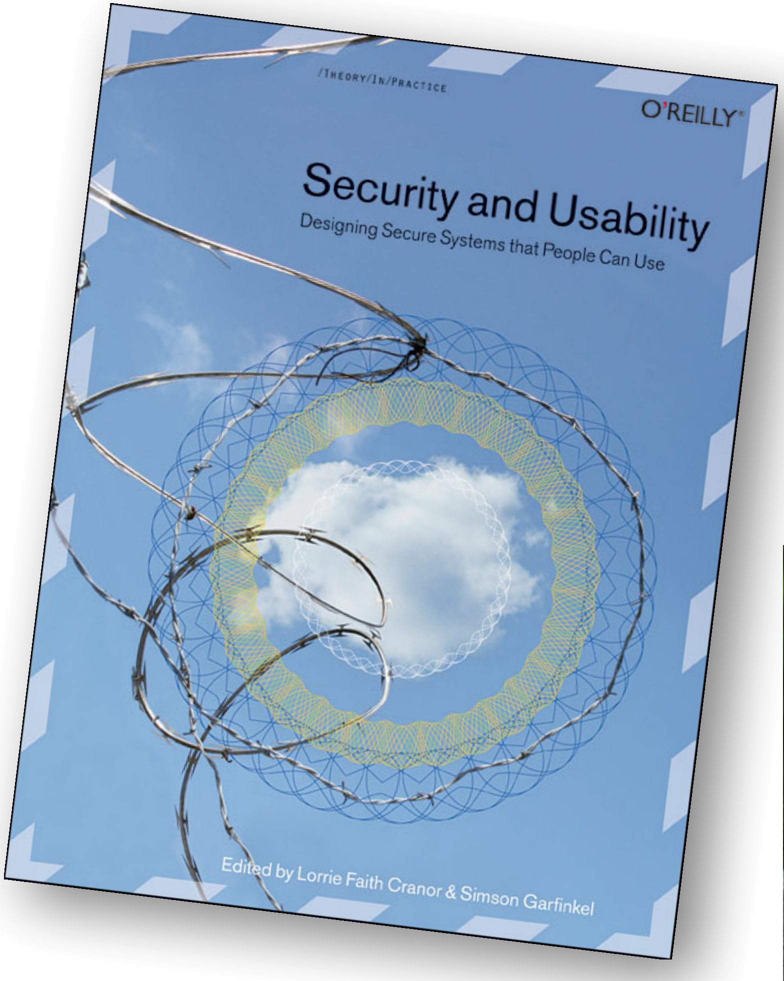
SOUPS

Symposium On Usable Privacy and Security

2018

https://www.usenix.org/conference/soups2018

Want to learn more?



/THEORY/IN/PRACTICE

O'REILLY

Security and Usability

Designing Secure Systems that People Can Use

Edited by Lorrie Faith Cranor & Simson Garfinkel

SOUPS

Symposium On Usable Privacy and Security

2018

https://www.usenix.org/conference/soups2018

SP2

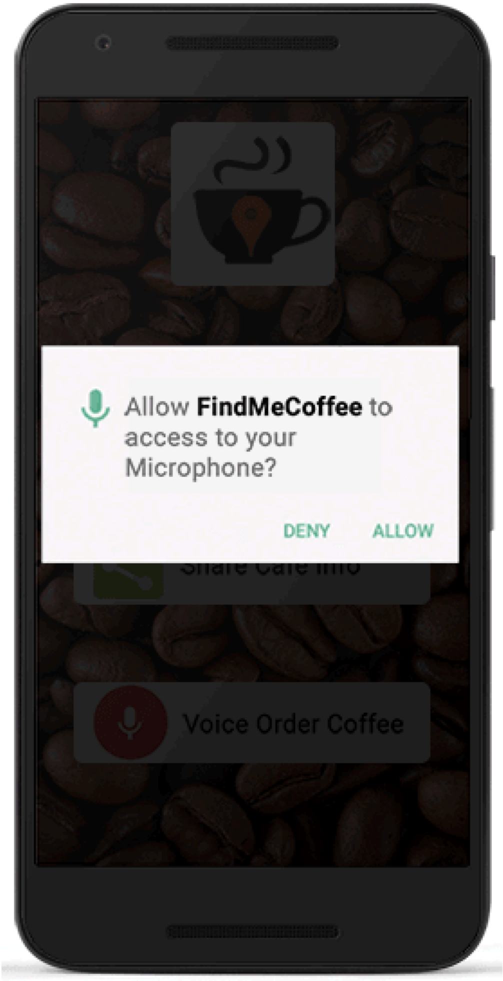
Security.Privacy.People

mmazurek@cs.umd.edu
dvotipka@cs.umd.edu

Case Study #4: Sensitive resource accesses and usage context

https://www.cs.umd.edu/~micinski/apptracer-2017.pdf

When is it ok for an app to access sensitive data?

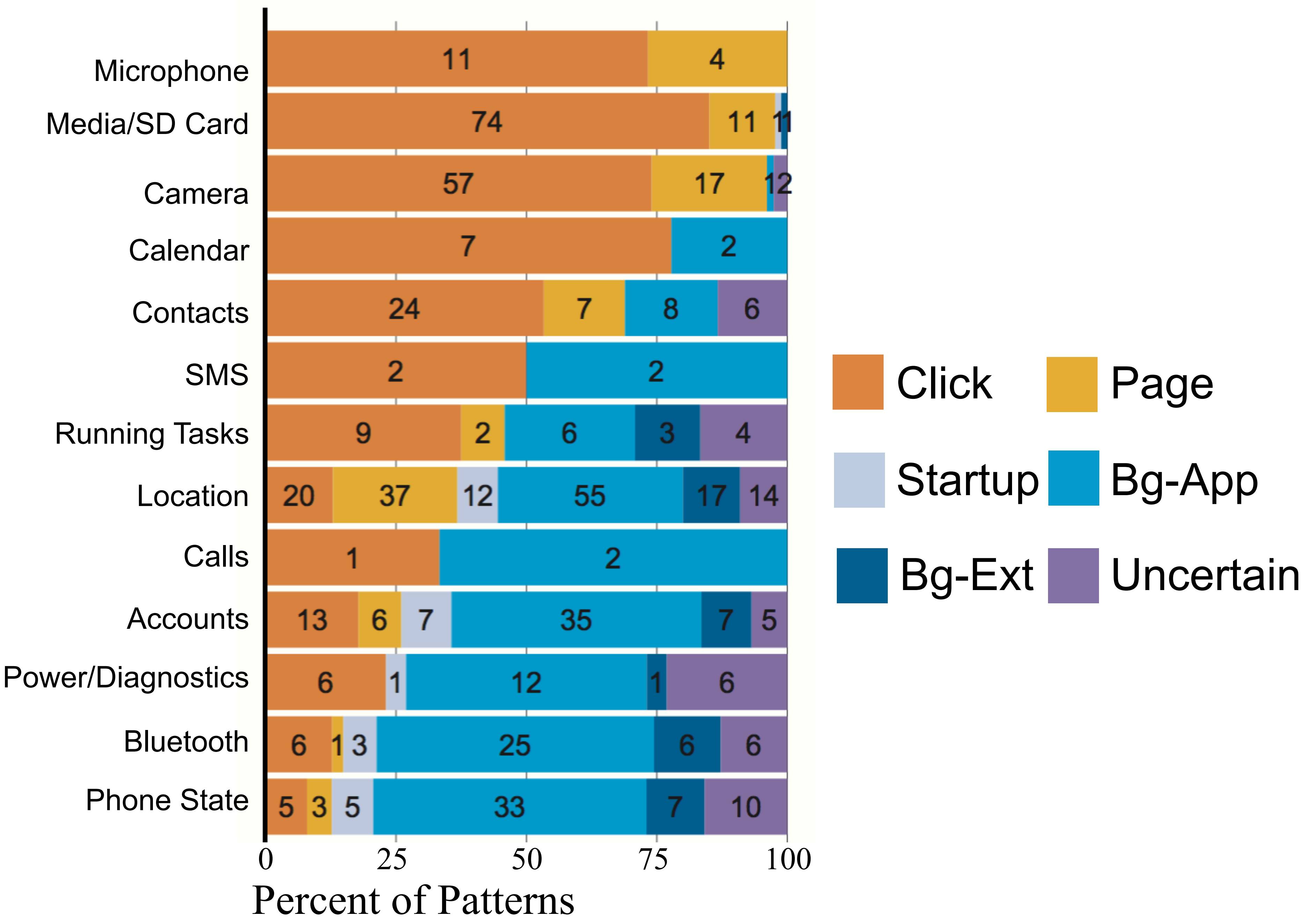


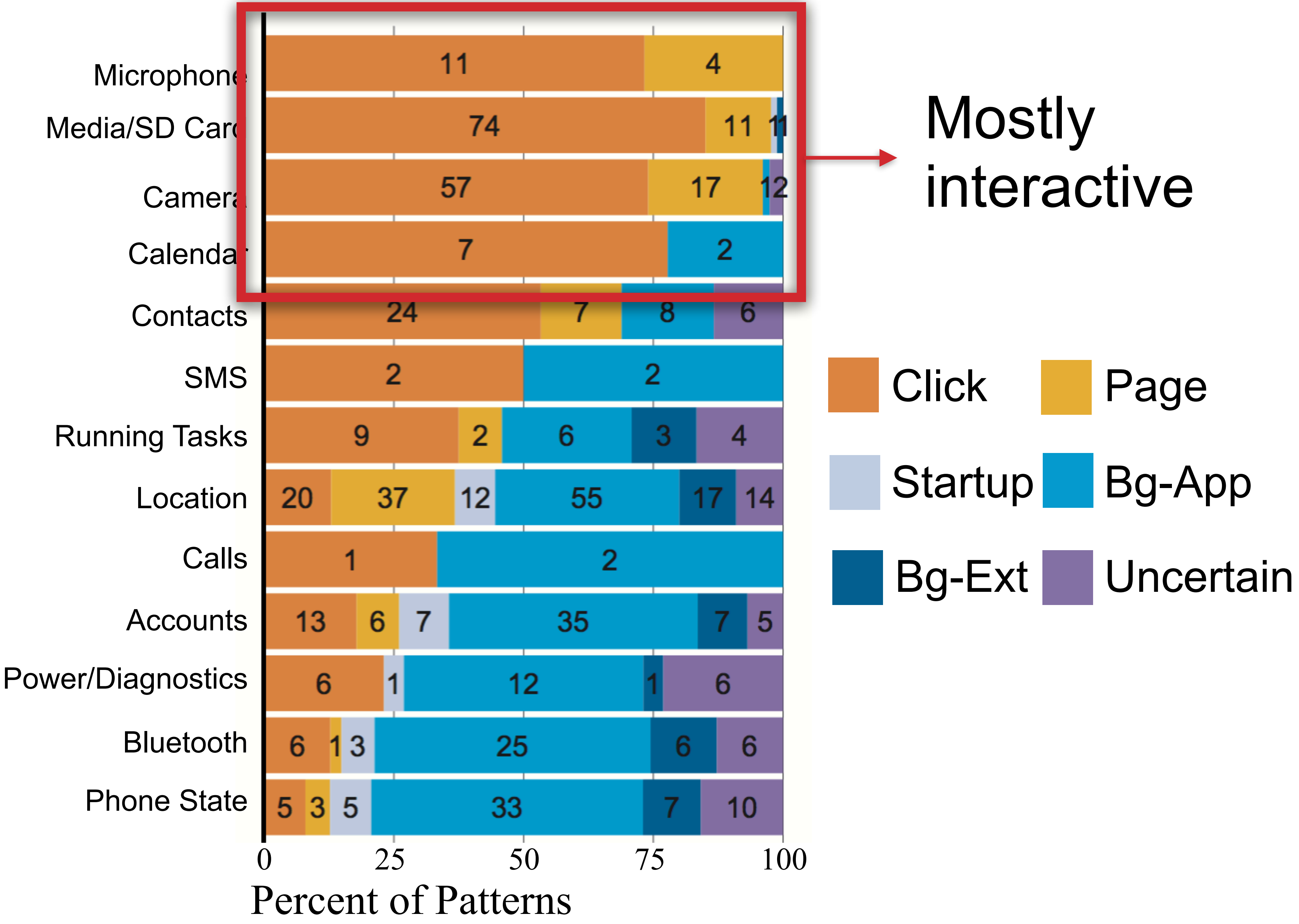
Allow **FindMeCoffee** to access to your Microphone?

[Micinski et. al, CHI 2017]

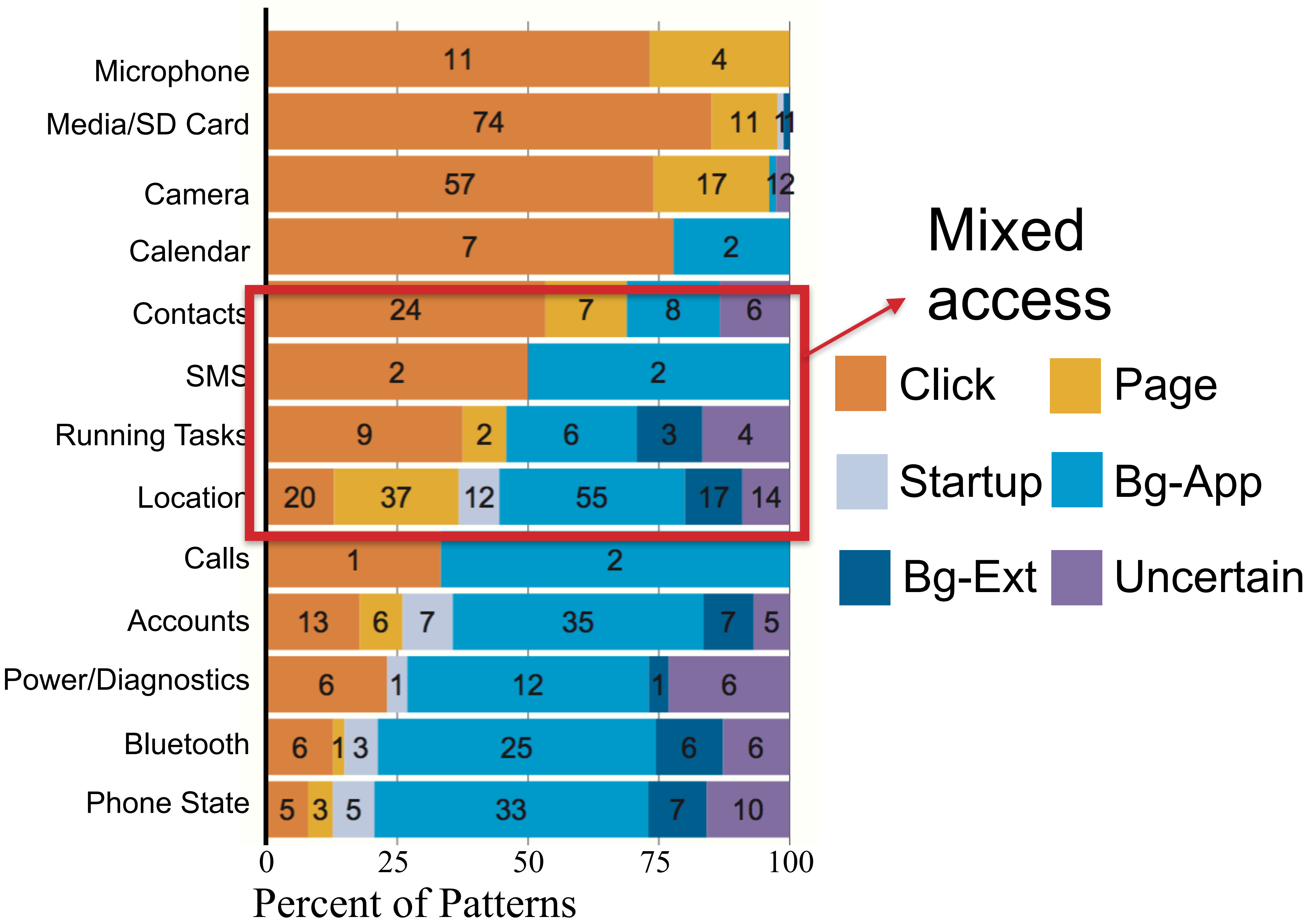
Experimental setup

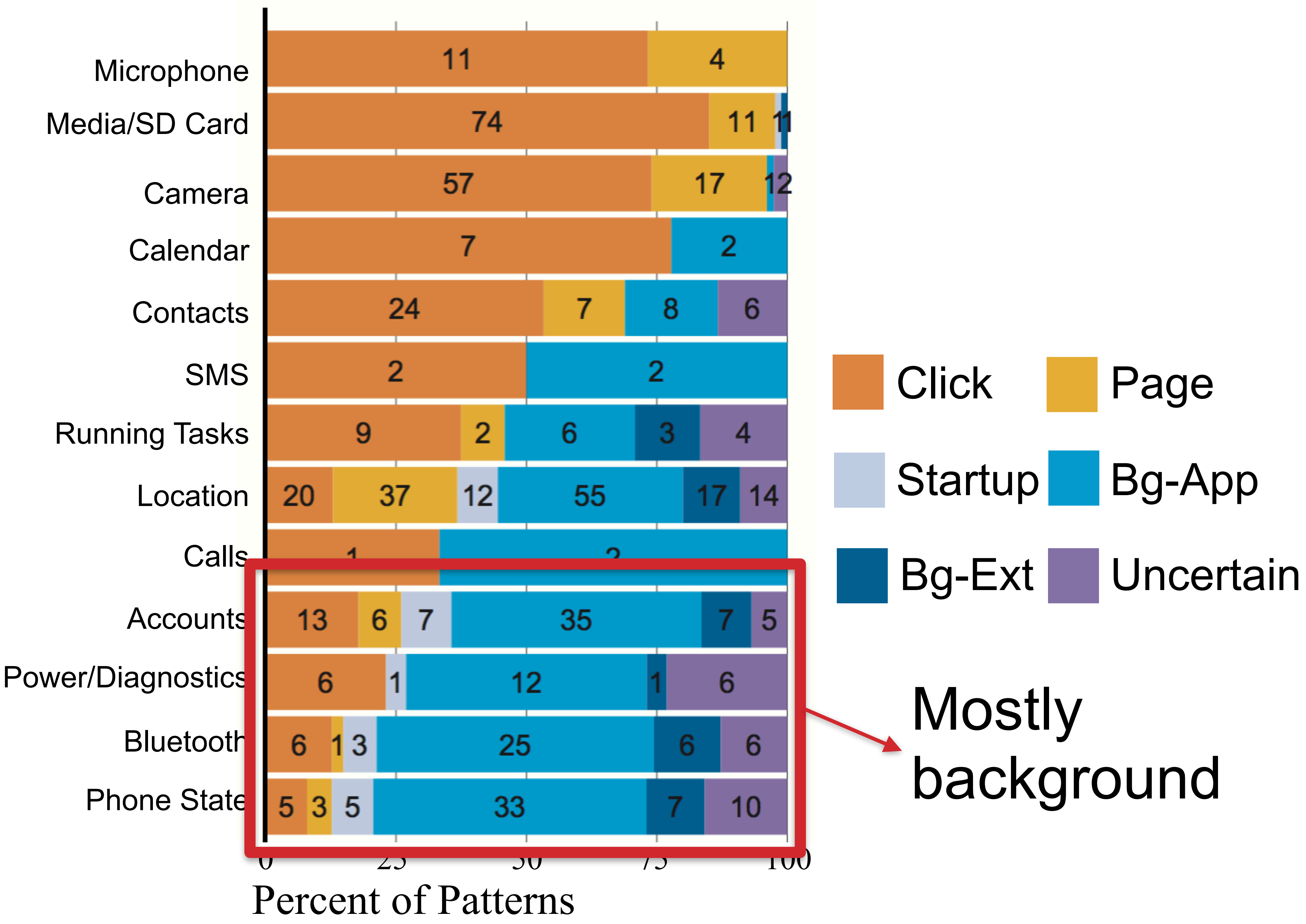
- Study #1:
  - Analyze 150 top apps
  - Determine how apps actually use resources
- Study #2:
  - Show MTurkers a variety of scenarios
  - See what they think the app is doing


Microphone
11
4
Media/SD Card
74
11
1
1
Camera
57
17
1
2
Calendar
7
2
Contacts
24
7
8
6
SMS
2
2
Running Tasks
9
2
6
3
4
Location
20
37
12
55
17
14
Calls
1
2
Accounts
13
6
7
35
7
5
Power/Diagnostics
6
1
12
1
6
Bluetooth
6
1
3
25
6
6
Phone State
5
3
5
33
7
10
0
25
50
75
100
Percent of Patterns
Click
Page
Startup
Bg-App
Bg-Ext
Uncertain

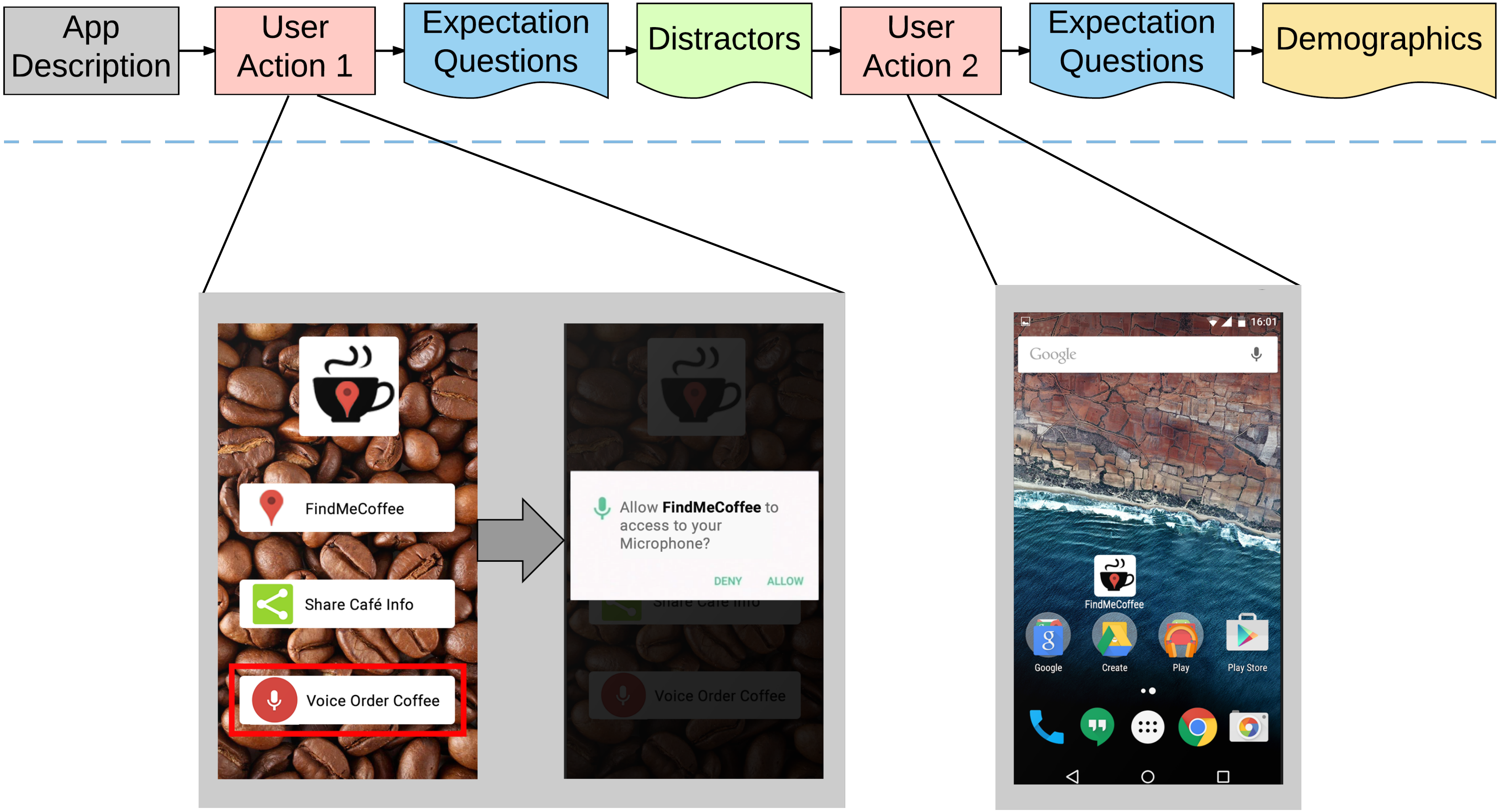


Mostly interactive





Mostly background



App Description → User Action 1 → Expectation Questions → Distractors → User Action 2 → Expectation Questions → Demographics

Allow **FindMeCoffee** to access to your Microphone?

Interactivity v. Expectation

- The more interactive the pattern, the more likely the user is to expect access
  - A resource access after a click was 106 times more expected than when no interaction shown

- Explicit authorization also shows significant increase

Effect of Prior Access

- Prior event of a click not significantly different from no interaction

- More likely to expect background access when prior event was not associated with user interaction

- *First Use* not significantly different from *Never* for second access
    - *First Use* may condition users to expect a single access