

Security and human behavior

Some material from Lorrie Cranor, Mike Reiter, Rob Reeder, Blase Ur

In this lecture ...

- Overview
- Minimizing effort
- Case studies
 - Password expiration, security images, password meters, implantable devices

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.”

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

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

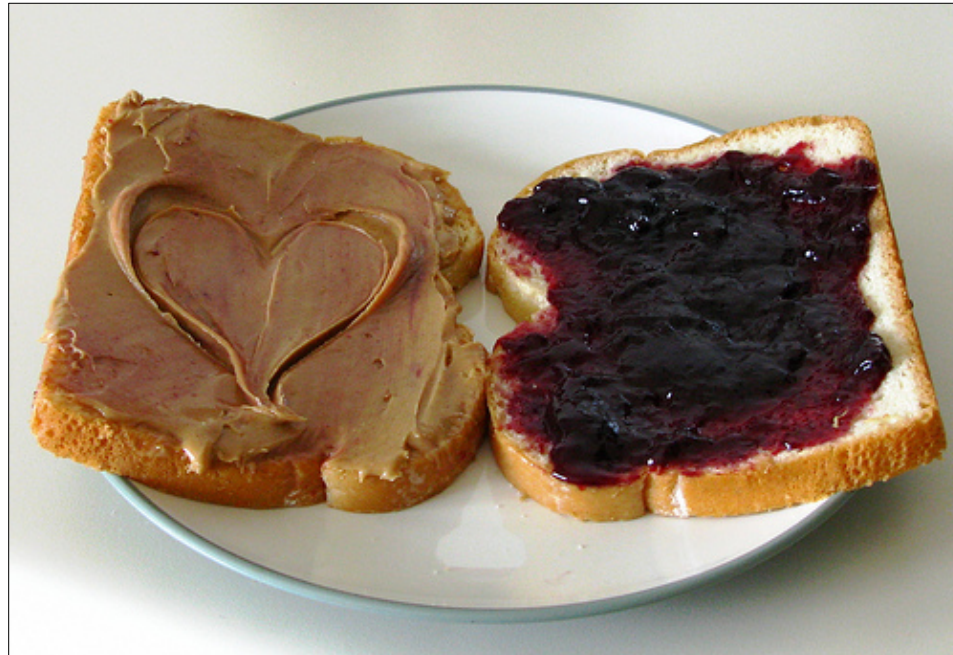
And one more ...

"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
2014**

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

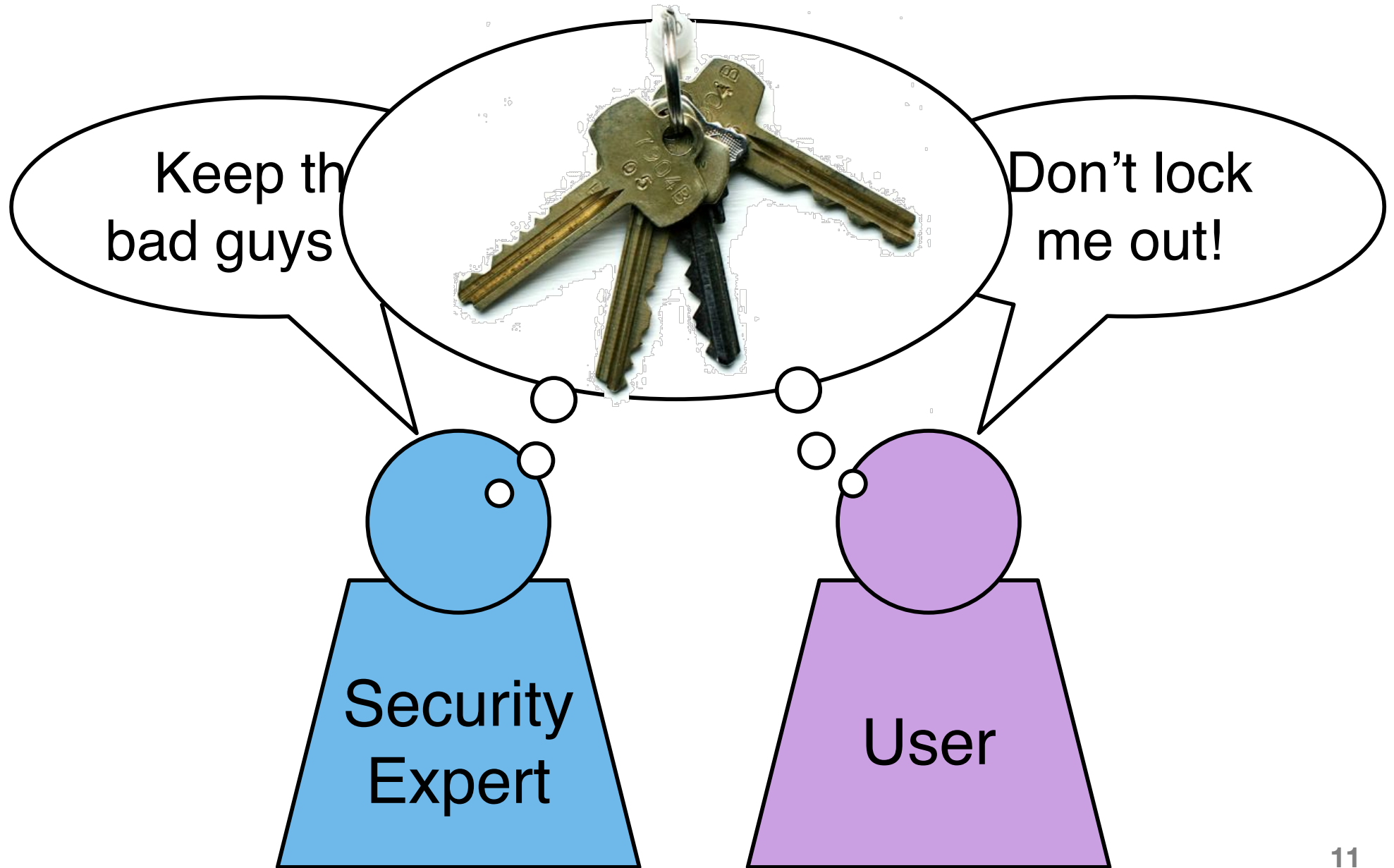
- Security is a **secondary task**
 - Users are trying to get something else done
- Security concepts are **hard**
 - Viruses, certificates, SSL, encryption, phishing
- Human capabilities are **limited**

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**



Key challenges

- Security is a **secondary task**
- Security concepts are **hard**
- Human capabilities are **limited**
- **Misaligned priorities**
- **Active adversaries**
 - Unlike ordinary UX

Twitter: W

http://twitter.access-logins.com/login/


Tools Media

Select Language ...

twitter

What is Twitter?

What? Why? How?



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?**

[Watch a video!](#)

Please sign in

user name or email address:

password:

Remember me [Sign In >](#)

[Forgot password? Click here.](#)

Already using Twitter from your phone? [Click here.](#)

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

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

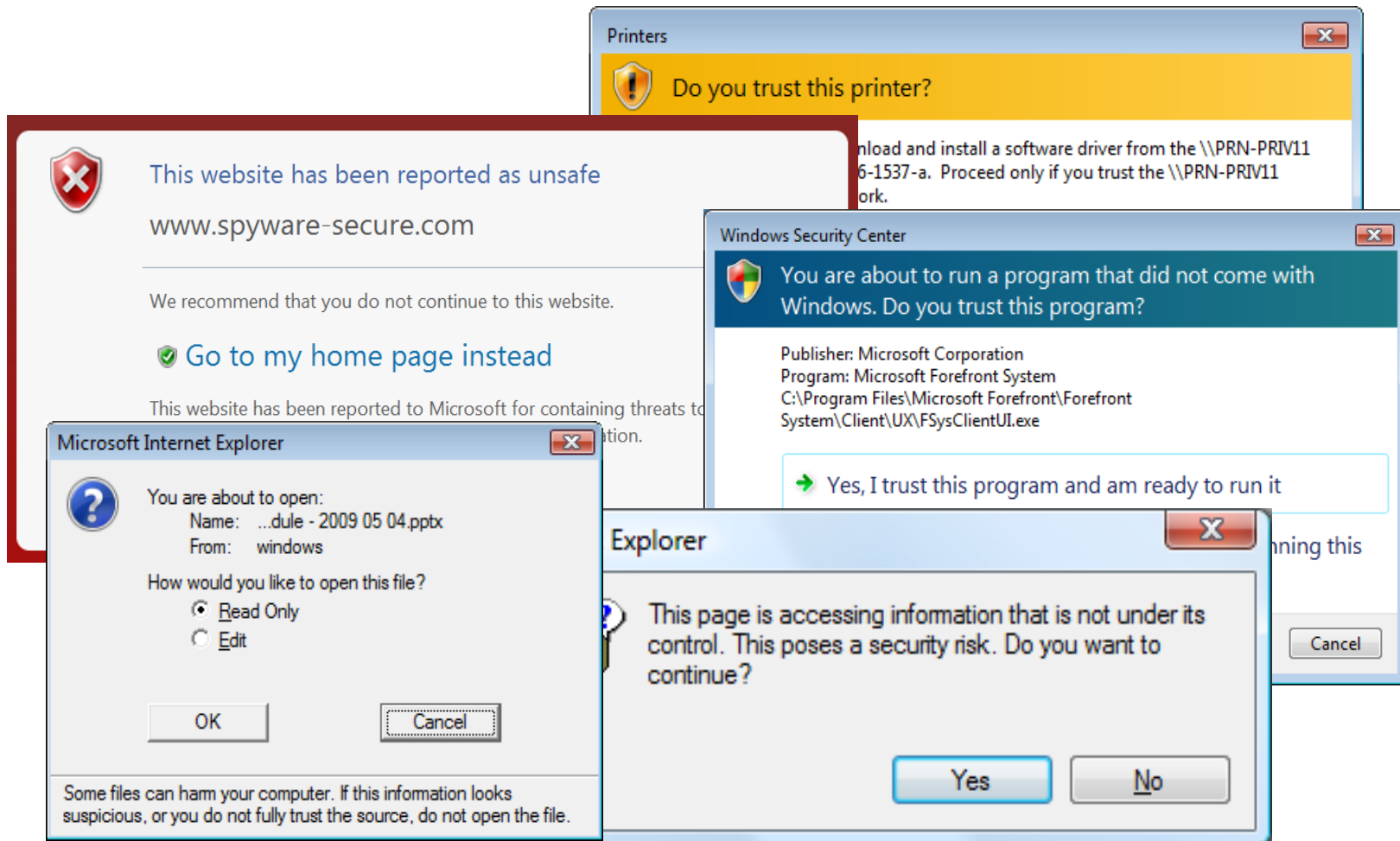
- Score:
 - 1 for Abraham Lincoln
 - +1 for Abraham Lincoln facing right
 - +1 for "Liberty"
 - +1 for "Liberty" to Abe's left
 - +1 for "In God We Trust"
 - +1 for "In God We Trust" over Abe's head
 - +1 for the year
 - +1 for the year to Abe's right
 - Extra credit: +1 for the mint letter under the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



Lessons from Abe

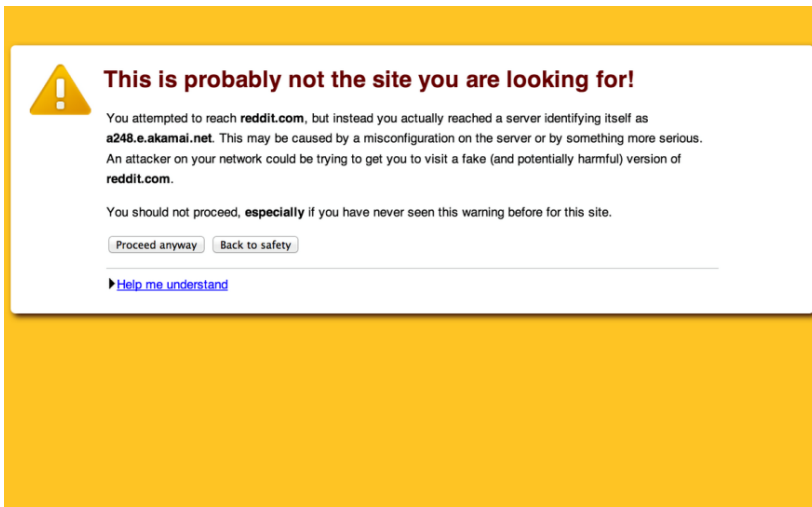
- You've probably seen hundreds of pennies
 - And yet, this is hard
- Memory limitations
 - Remembering a penny isn't important, unless you take this quiz!
- Habituation
 - You see it so often, you don't remember it anymore

Habituation to warnings

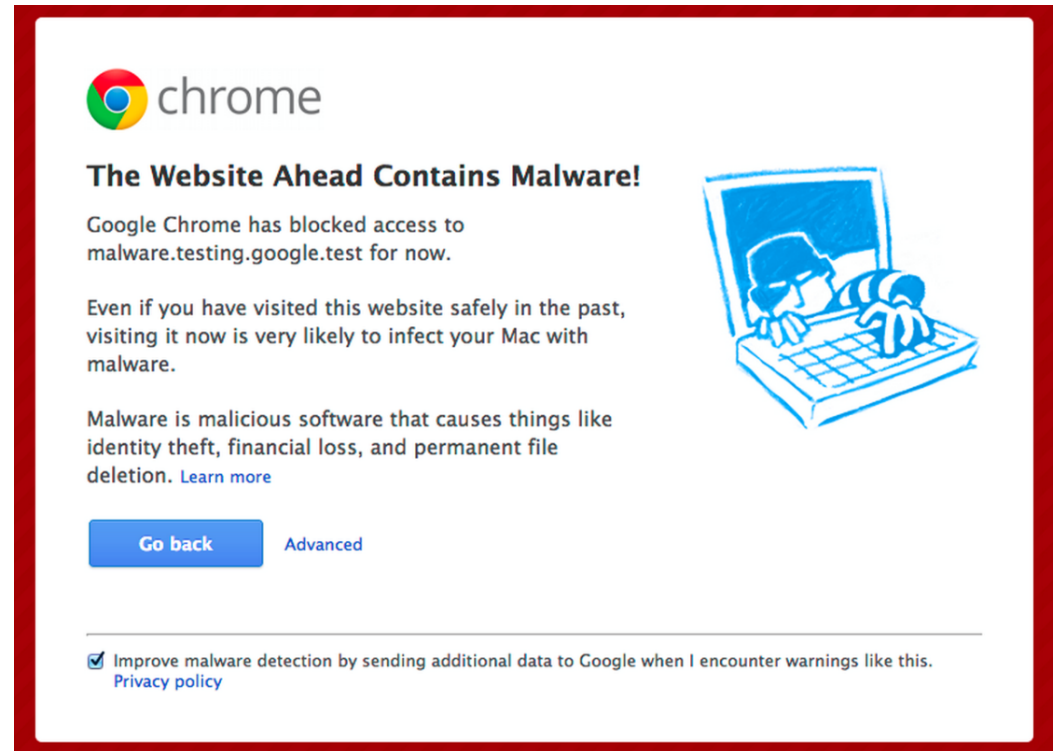




If it's important, make it stand out



SSL warning; risk low;
yellow background

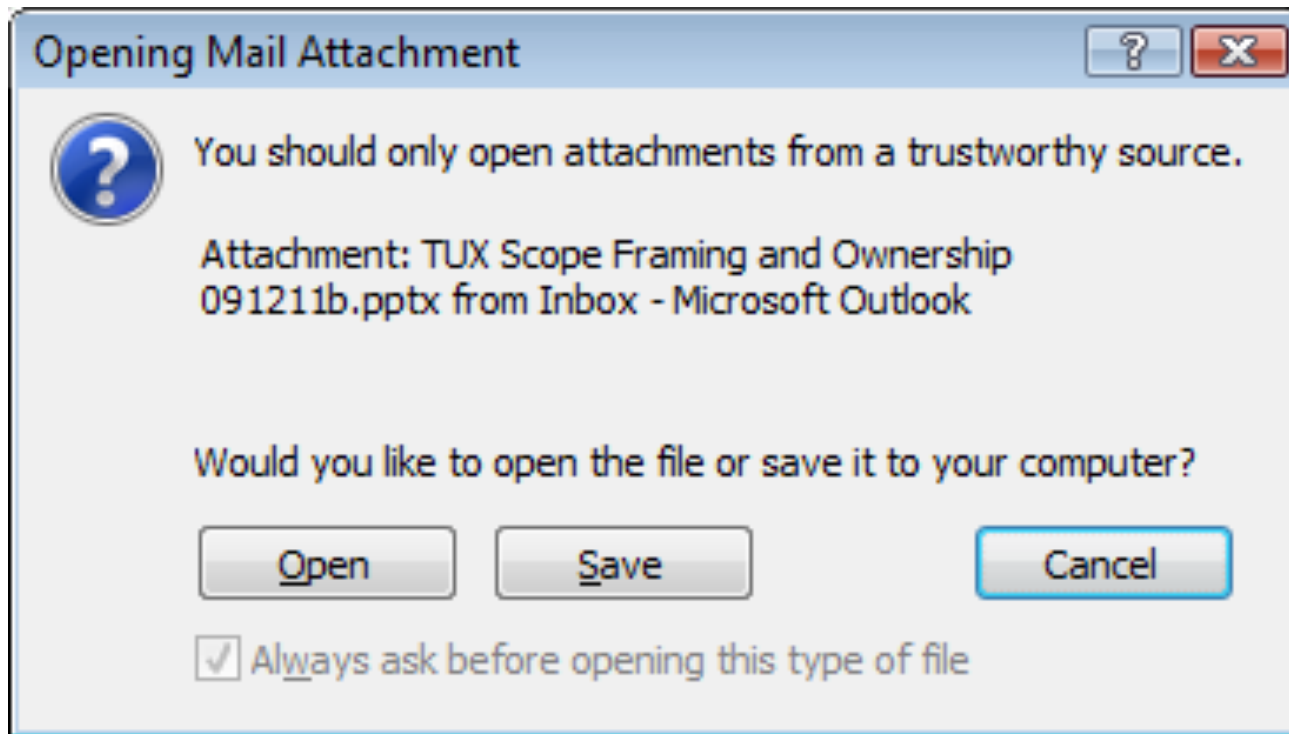


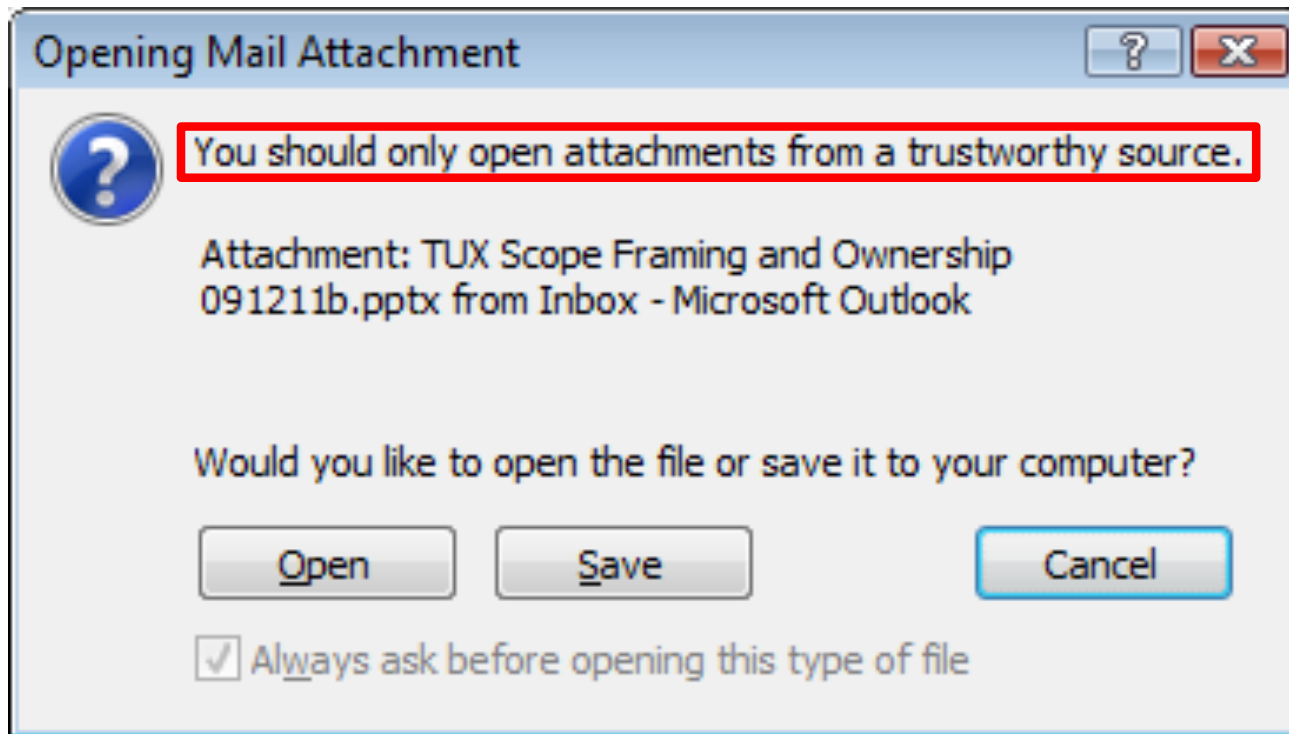
Malware warning; risk very high;
red background

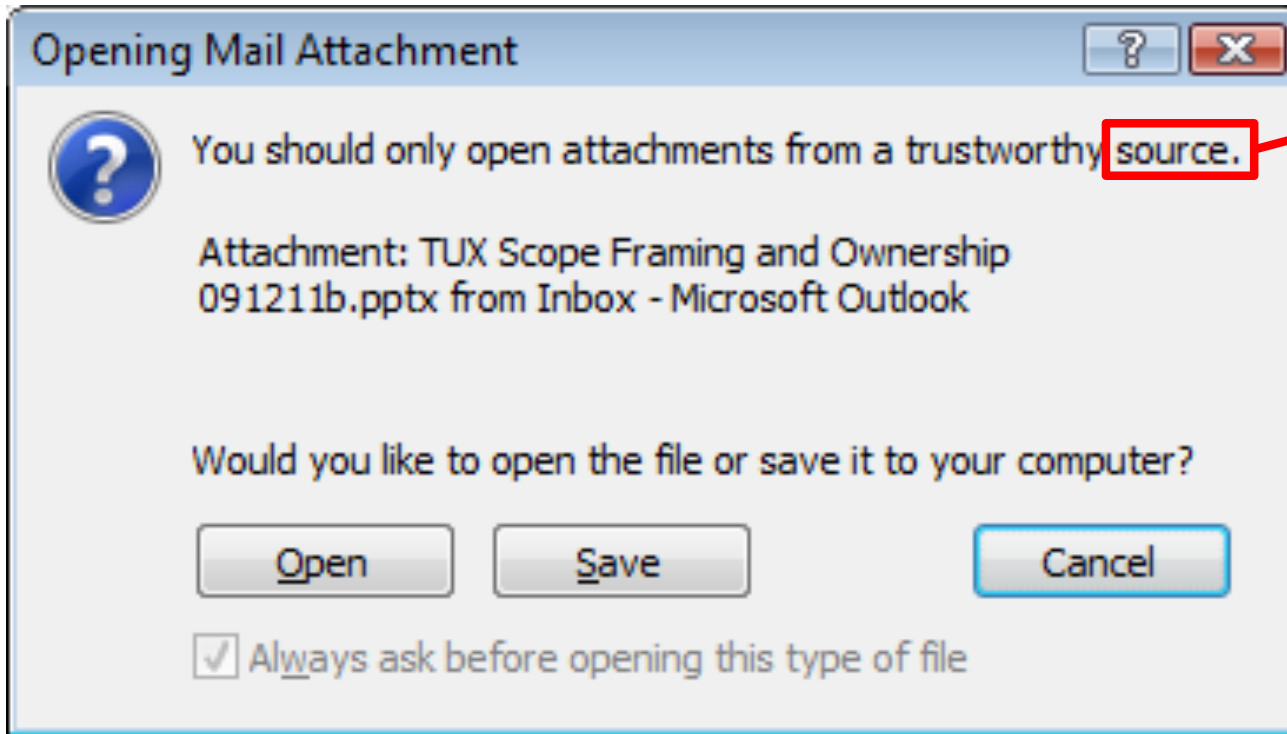
MINIMIZING EFFORT

People are economical

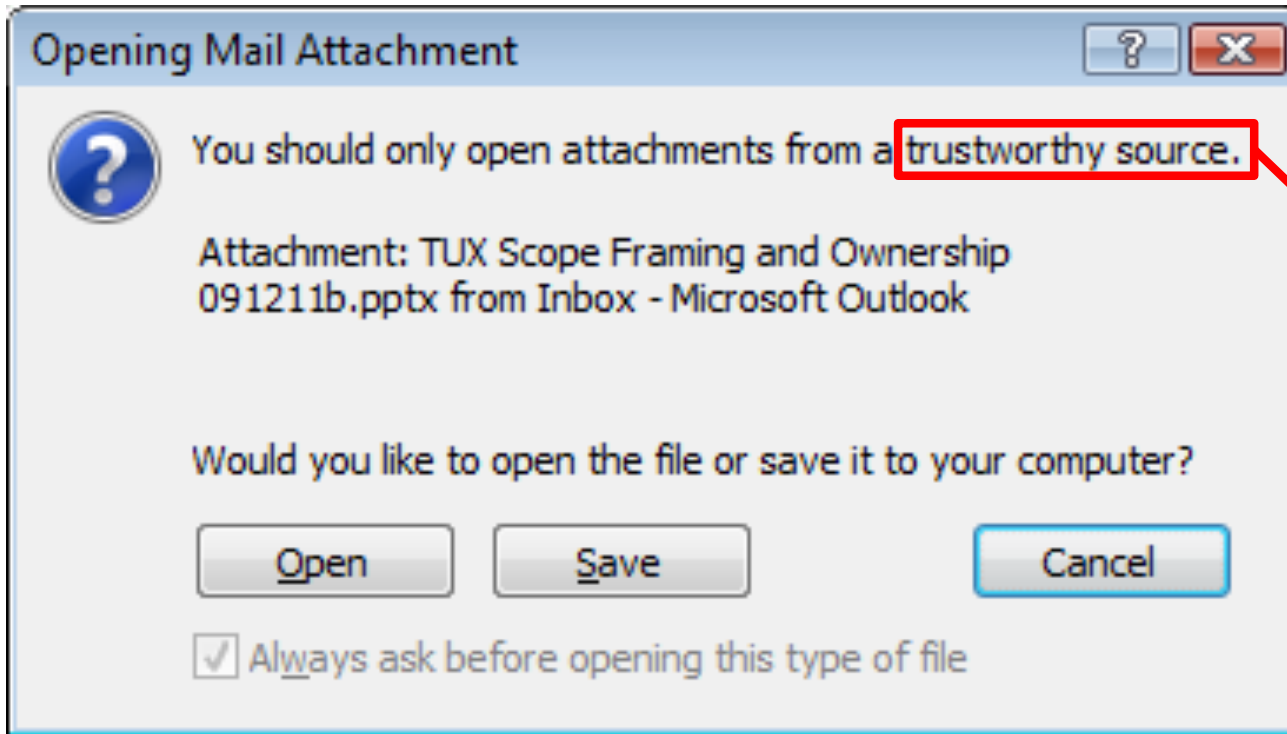
- Given two paths to a goal, they'll take the shorter path
- More steps = less likely they'll be completed
- Can they figure out what to do?
 - Too hard = give up and take easiest path





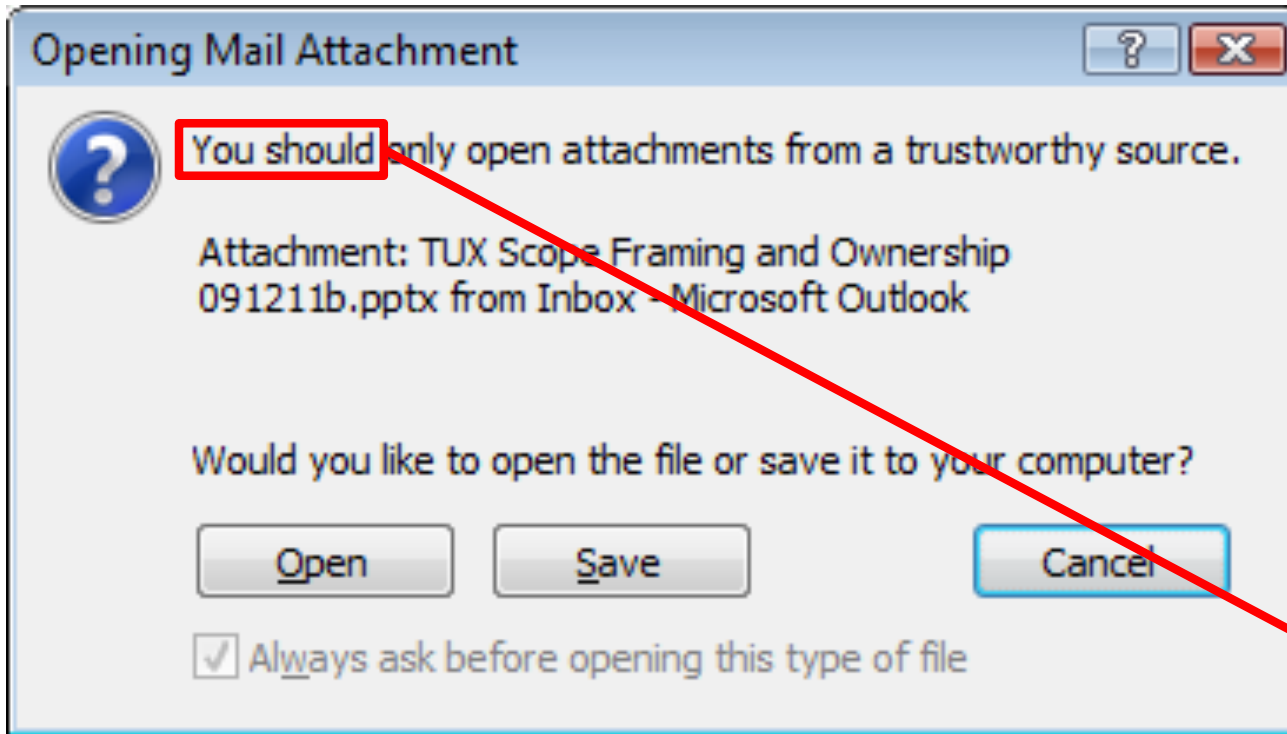


What's the source of this attachment?



What's the source of this attachment?

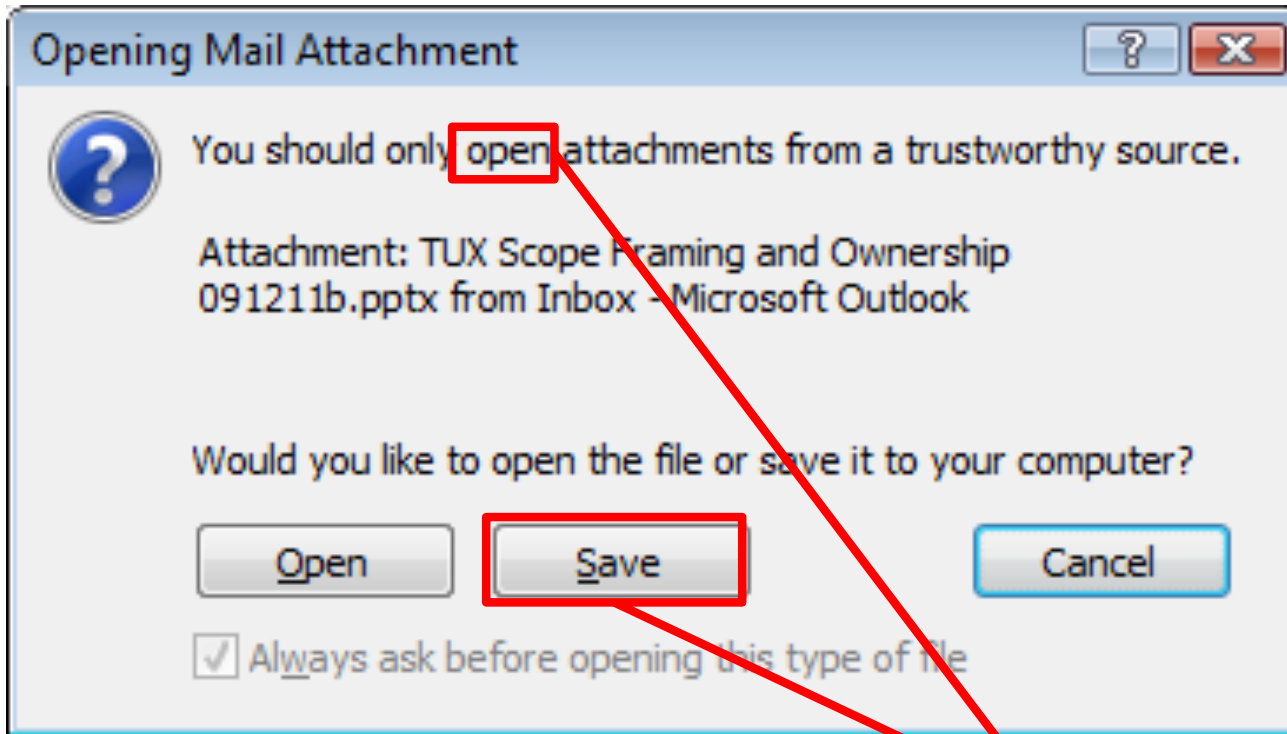
What makes a source trustworthy or not trustworthy?



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?

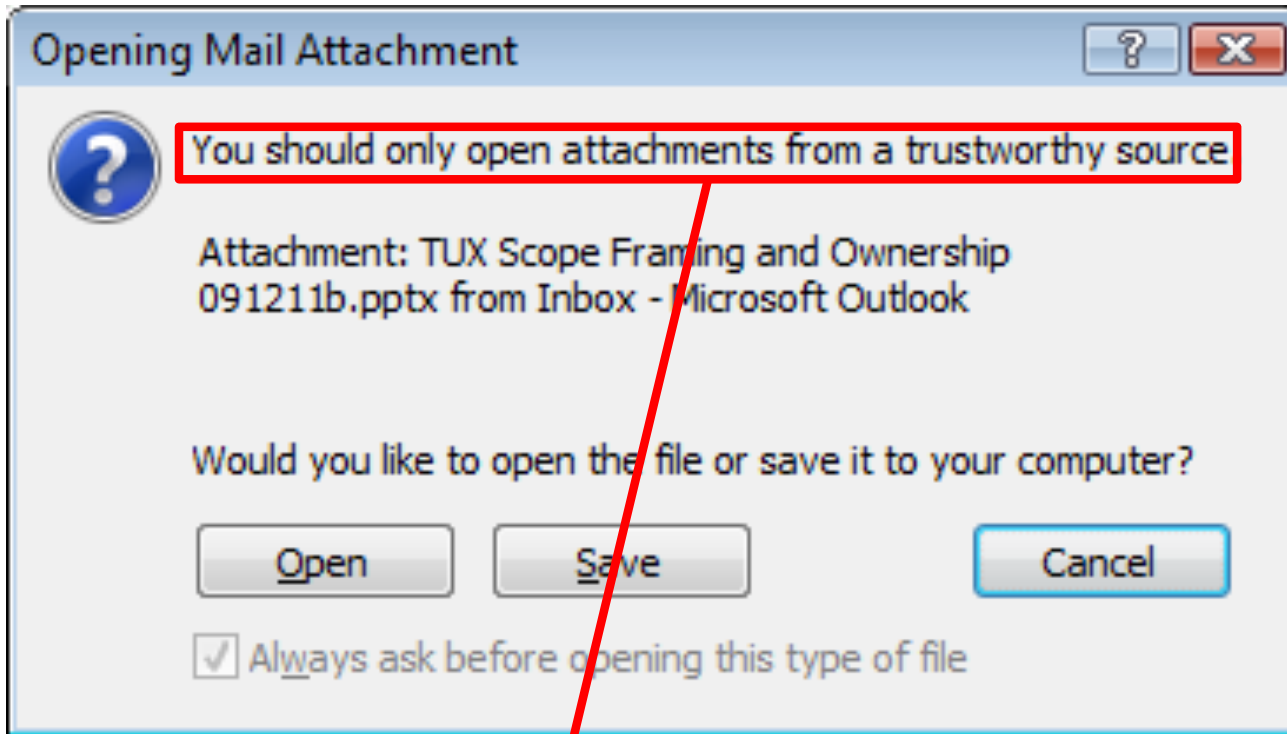


What's the source of this attachment?

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 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

What can go wrong when you don't consider human factors

CASE STUDIES

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**

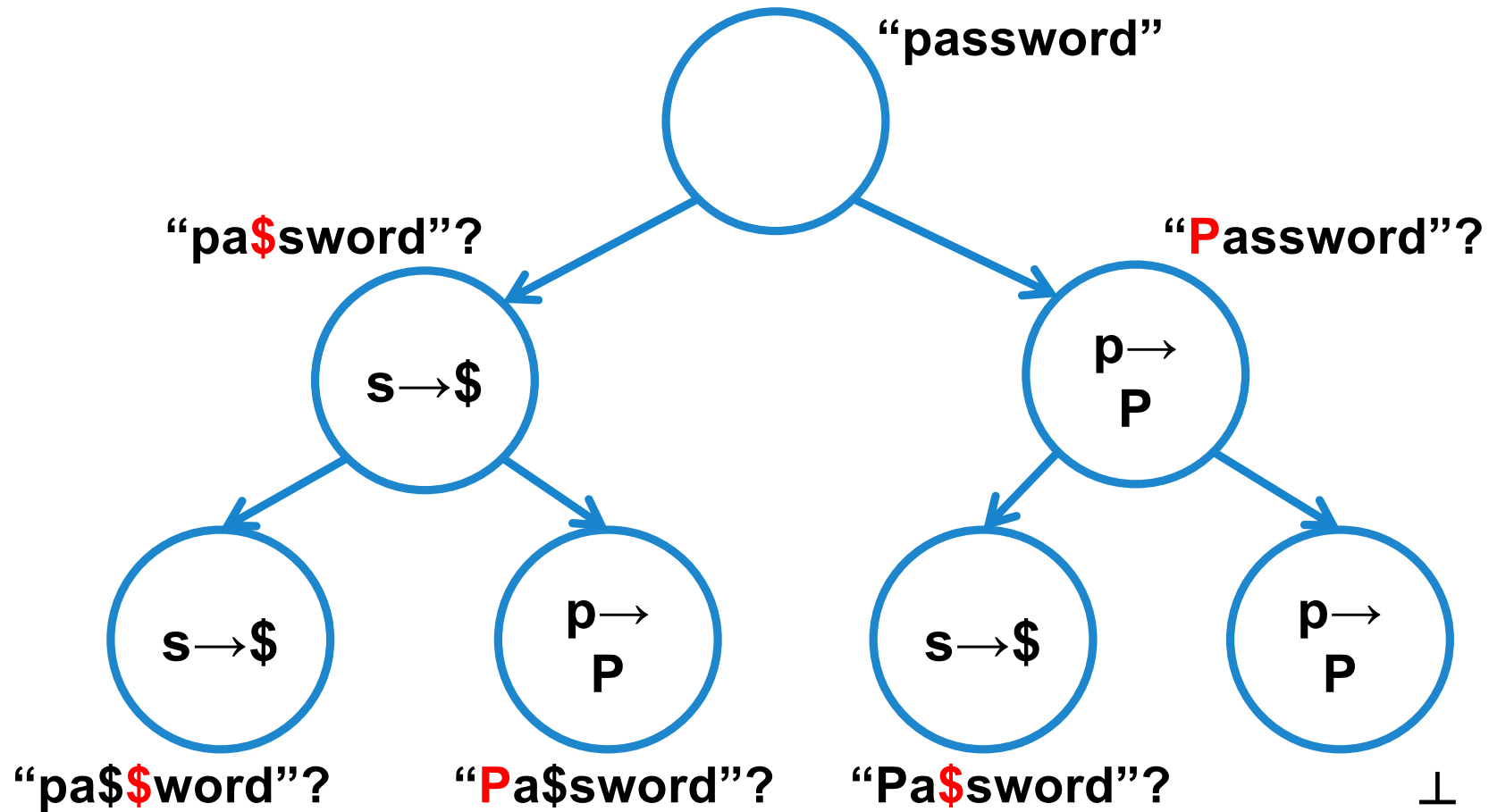
- Attackers can exploit the similarity of passwords in the same account to predict the future password based on the old ones

[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

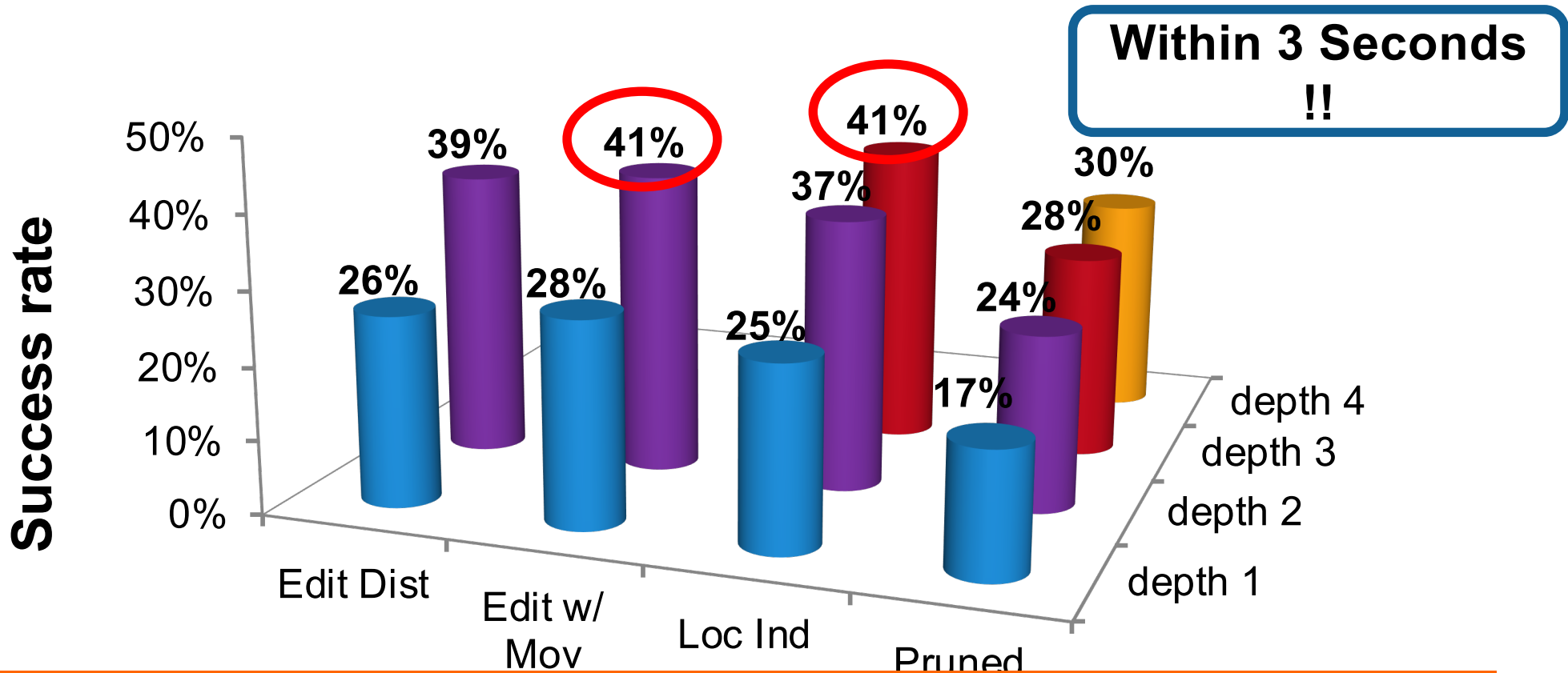
Location Independent Transforms

CATEGORY	EXAMPLE
Capitalization	tarheels#1 → tArheels#1
Deletion	tarheels#1 → tarheels1
Duplication	tarheels#1 → tarheels#11
Substitution	tarheels#1 → tarheels#2
Insertion	tarheels#1 → tarheels#12
Leet Transform	tarheels#1 → t@rheels#1
Block Move	tarheels#1 → #tarheels1
Keyboard Transform	tarheels#1 → tarheels#!

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

Complete Sign On

Verify Identity

Please verify that your Personal Security Image and Caption are correct

Step 1: Verify Your Personal Security Image and Caption

Is this your Personal Security Image?



Is this Your Caption?

Nice House

If you do not recognize your Personal Security Image & Caption then DO NOT enter your password and email us immediately at cmu-banking-research-study@ece.cmu.edu .

Step 2: Enter Password

User ID: tyutyu

Password: [Forgot Password?](#)

[Sign On](#)

Information Center

[Online Banking Service Agreement](#) *New*

Sign On Questions

[What is the Personal Security Image and Caption?](#)

[What should I do if I forgot my Personal Security Image and/or Caption?](#)

[What should I do if the wrong Personal Security Image and/or Caption is showing?](#)



Goal: Prevent phishing

Step 11 Verify Your Personal Security Image and Caption

Is this your Personal Security Image?



Is this Your Caption?

Nice House

If you do not recognize your Personal Security Image & Caption then DO NOT enter

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

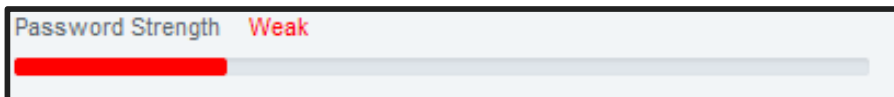
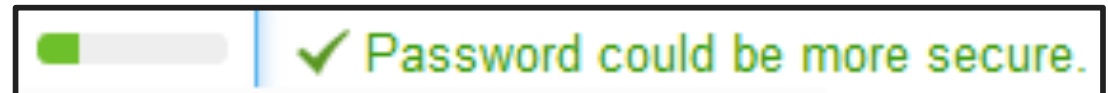
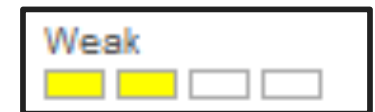
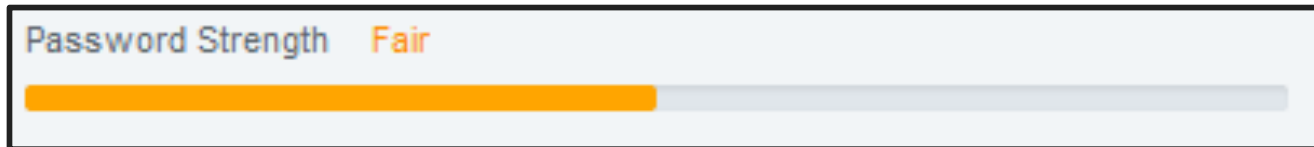
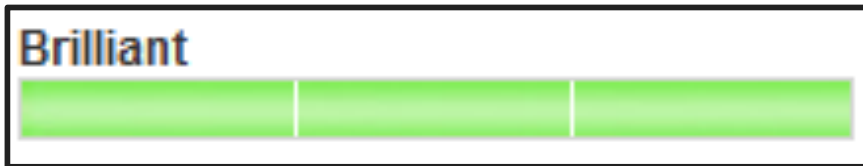
- 80-100% claimed they looked at the image, but:
- 73% entered passwords despite no image
- No significant differences by image type
- Users with stronger passwords logged in less often (65% to 80%)

Takeaway: Attention failure, misaligned priorities, misunderstanding security concepts

PASSWORD METERS AND MOTIVATING YOUR USERS

Password Meters ...

- ... come in all shapes and sizes



Experimental setup

- No meter
- Baseline (boring) meter
- Visual differences
 - Size, text only
- Dancing bunnies (wait and see)
- Scoring differences
 - Same password scores differently

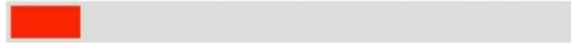
Conditions with Visual Differences

Type new password:

8-character minimum; case sensitive

Baseline meter

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



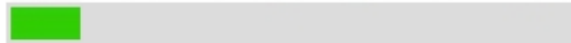
Three-segment

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.

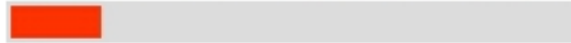
Conditions with Visual Differences

Type new password:

8-character minimum; case sensitive

Baseline meter

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



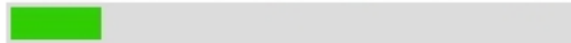
Three-segment

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:

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:

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:

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:

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.

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:

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:

8-character minimum; case sensitive

Baseline meter

Excellent!



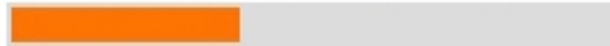
Half-score

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



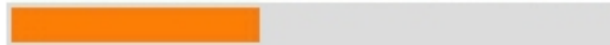
One-third-score

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:

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:

usernIX\$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:

usernIX\$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:

usernIX\$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:

usernIX\$e5WHYismyP4\$\$word99notGOODenough?

8-character minimum; case sensitive

Baseline meter

Excellent!



Half-score

Excellent!



One-third-score

Excellent!



Nudge-B16

Excellent.

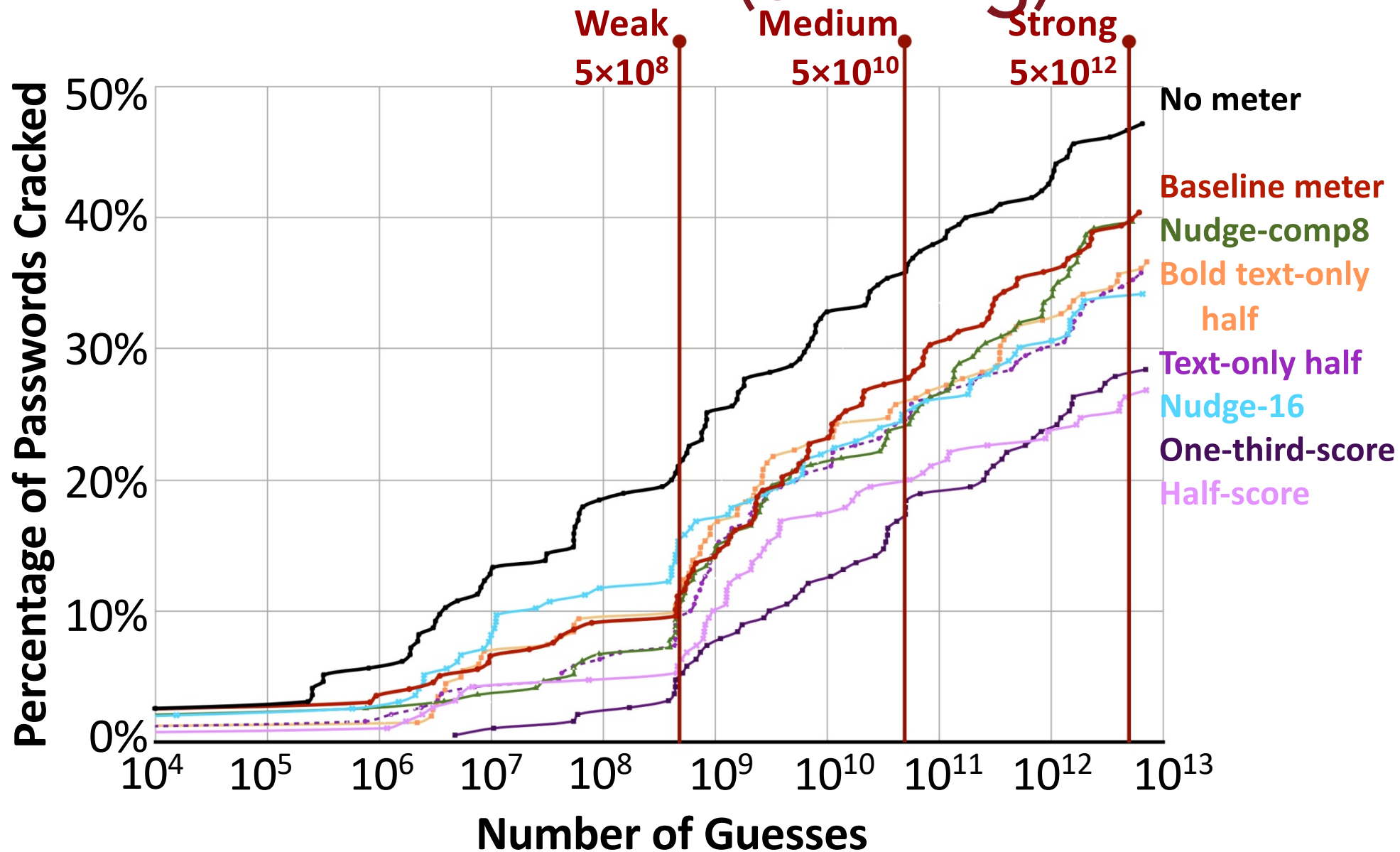


Nudge-Comp8

Excellent!



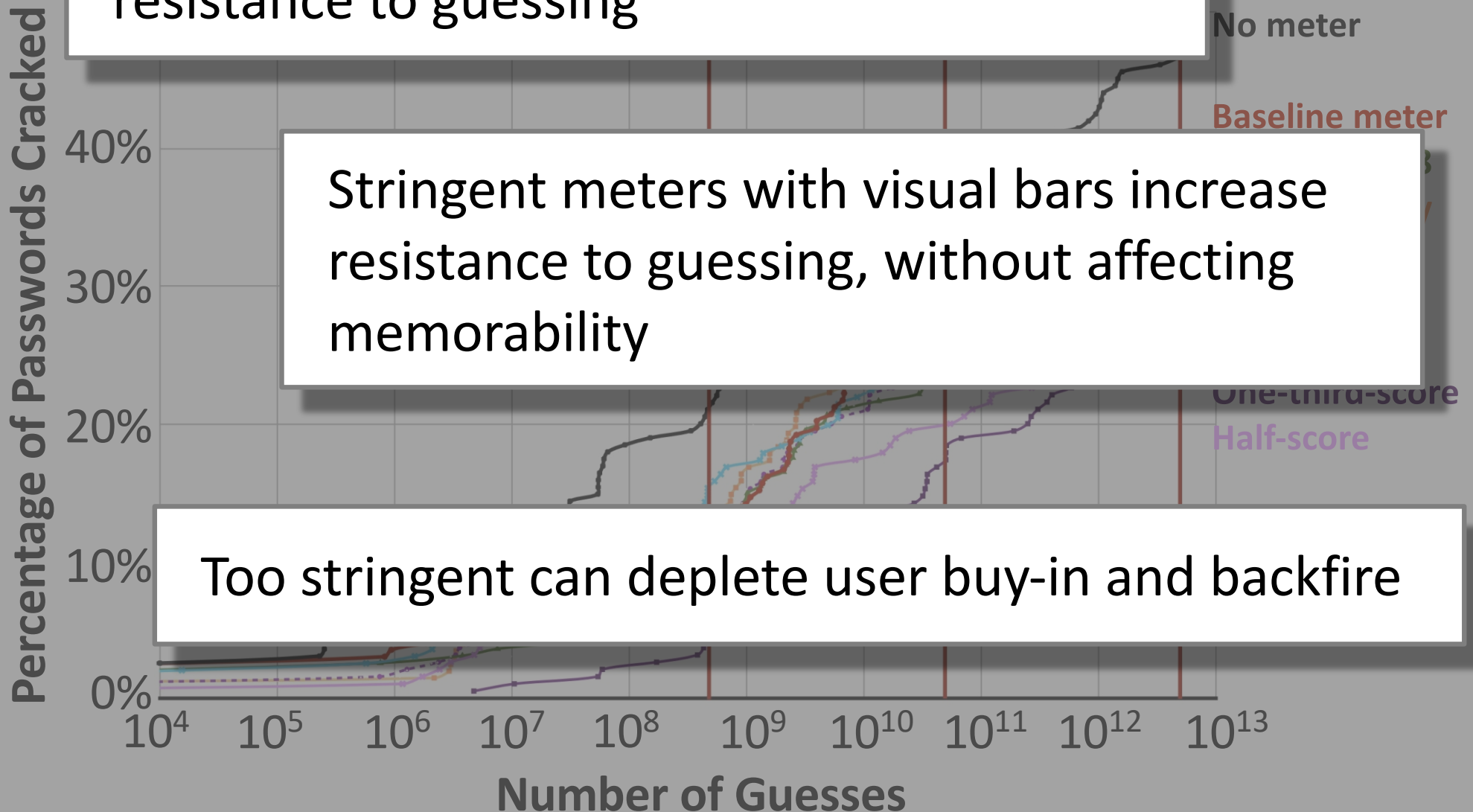
Password Meters (Scoring)



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



IMPLANTABLE DEVICES: BALANCING SECURITY AND OTHER VALUES

Implantable medical devices

- E.g., pacemakers, implantable defibrillators
- Increasingly, wireless comms:
 - Configure non-invasively
 - Report status and alerts automatically
- 2008: One model can be hacked wirelessly
 - Modify settings, steal private info, send large shock

A security paradox

- Authorized clinical access: ALWAYS
- Unauthorized access: NEVER
- ... EXCEPT:
 - Emergency access for EMTs, unknown docs/hospitals
- Non-goal: Protection given long physical access

Brainstorm: Potential solutions?

Some potential solutions

- Passwords
 - Available via some broad medical database
 - Carried in wallet
 - Carried on medical alert bracelet
 - Visible or UV tattoo

More potential solutions

- Proximity device
 - “Master key” kept in doctor’s offices, hospitals
 - Locked when wearing bracelet/wearable
 - Unlocked when wearing bracelet/wearable
- Automated detection of emergency condition

Interview study: Result highlights

	Liked (%)	Disliked (%)	Would Choose (%)
Password on bracelet	0	27	0
Visible tattoo	9	55	9
UV tattoo	18	27	18
Unlock if bracelet absent	0/45	36/27	0/27
Proximity master key	27	0	27
Emergency detection	27	18	27

N = 11