Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords

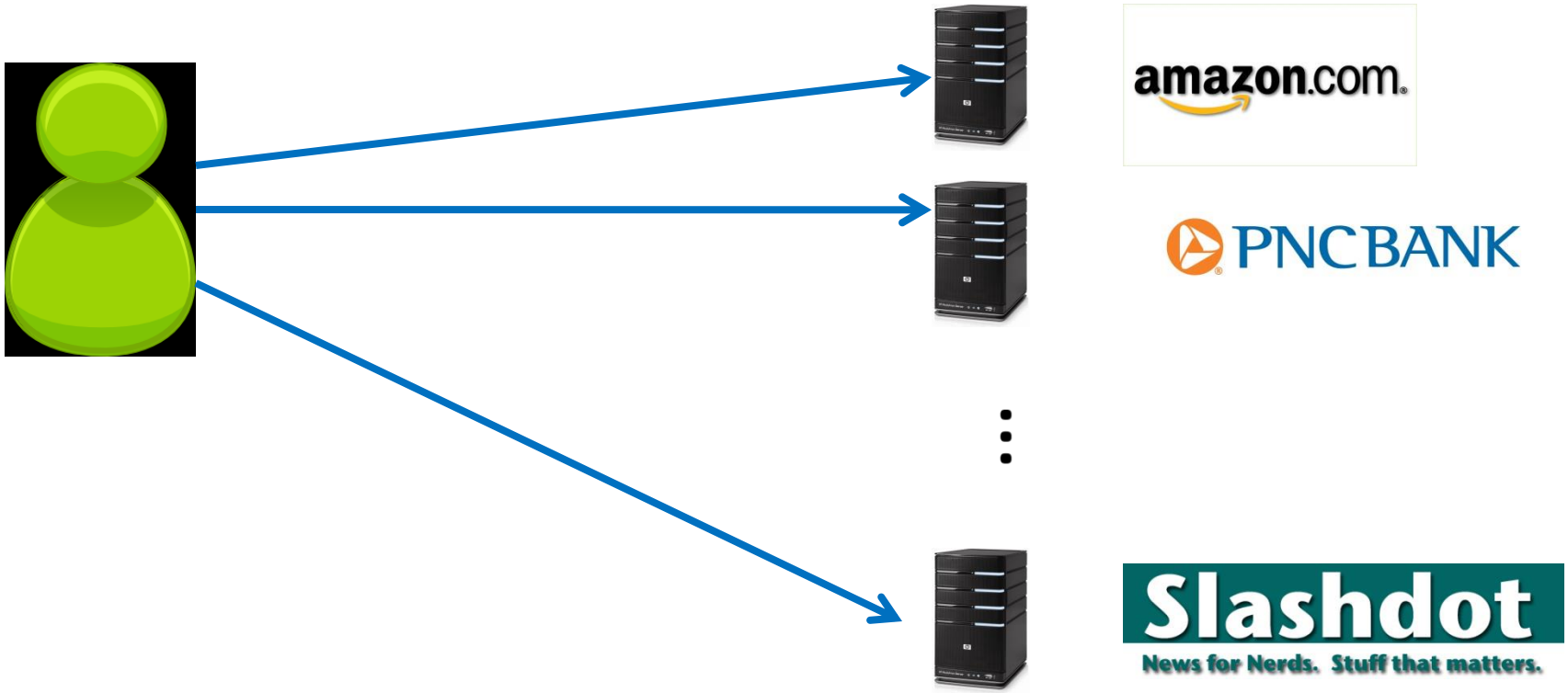


Jeremiah Blocki
Saranga Komanduri
Lorrie Cranor
Anupam Datta

Carnegie Mellon University

NDSS 2015

Motivation

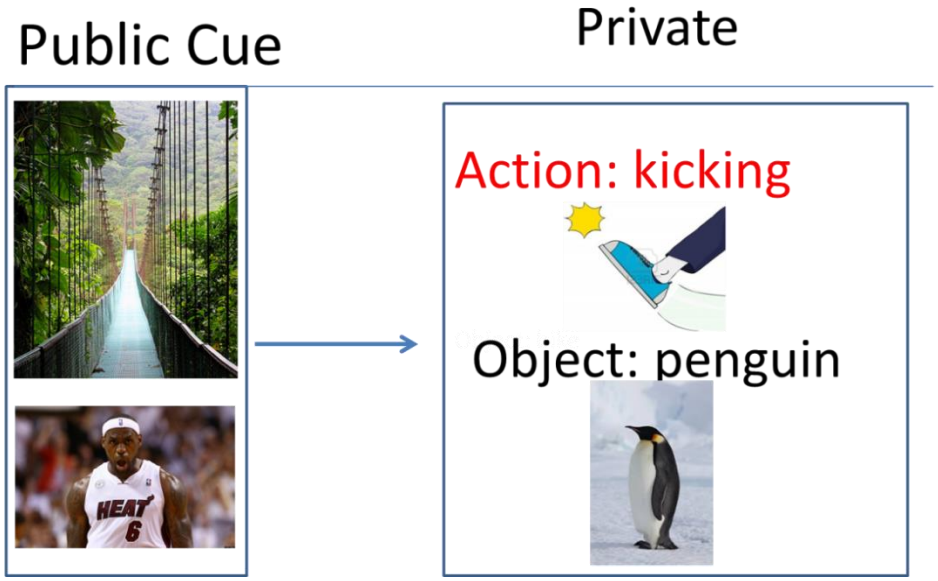

amazon.com
PNC BANK
Slashdot
News for Nerds. Stuff that matters.

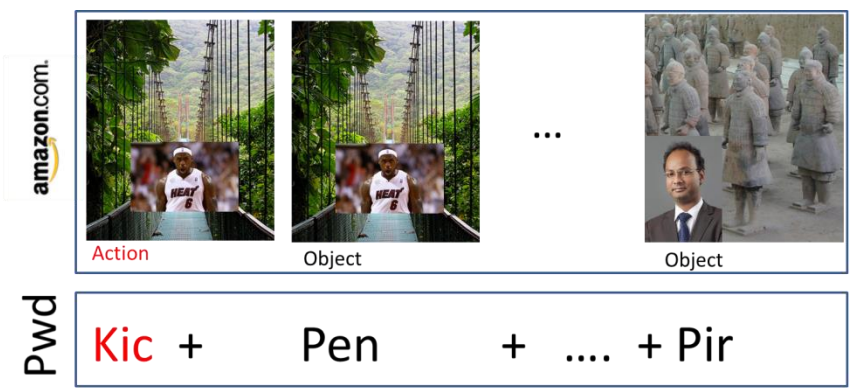
Usability Problem

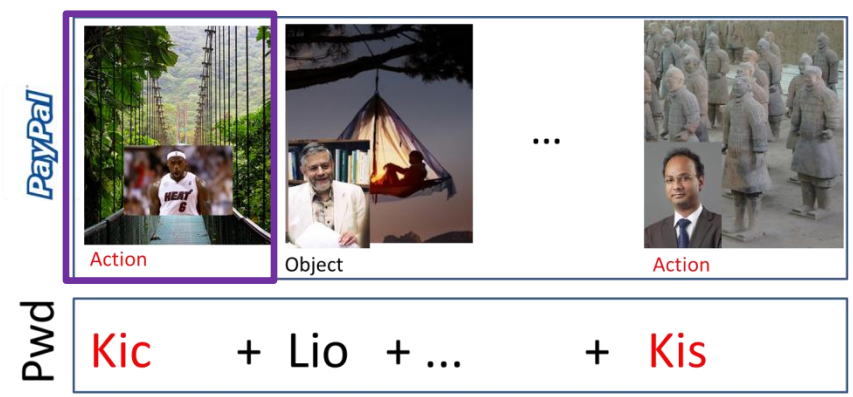
Security Problem

- Password breaches at major companies have affected millions of users.

Previous Work: Shared Cues







Source: Naturally Rehearsing Passwords [BBD13]

Previous Work: Shared Cues

Combinatorial Design: Each pairs of accounts has at most γ secret stories in common.

Source: Naturally Rehearsing Passwords [BBD13]

Previous Work: Shared Cues

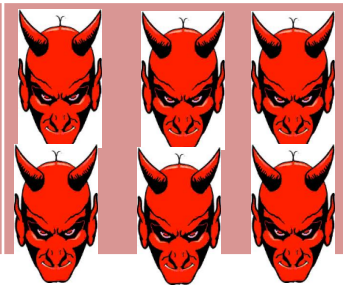
PAO Stories	#Passwords	Security
4	14	

Previous Work: Shared Cues

PAO Stories	#Passwords	Security
4	14	

Adversary with one password is unlikely to crack any other password

Previous Work: Shared Cues

PAO Stories	#Passwords	Security
4	14	
7	75+	
15	75+	
43	75+	

User Study Goals

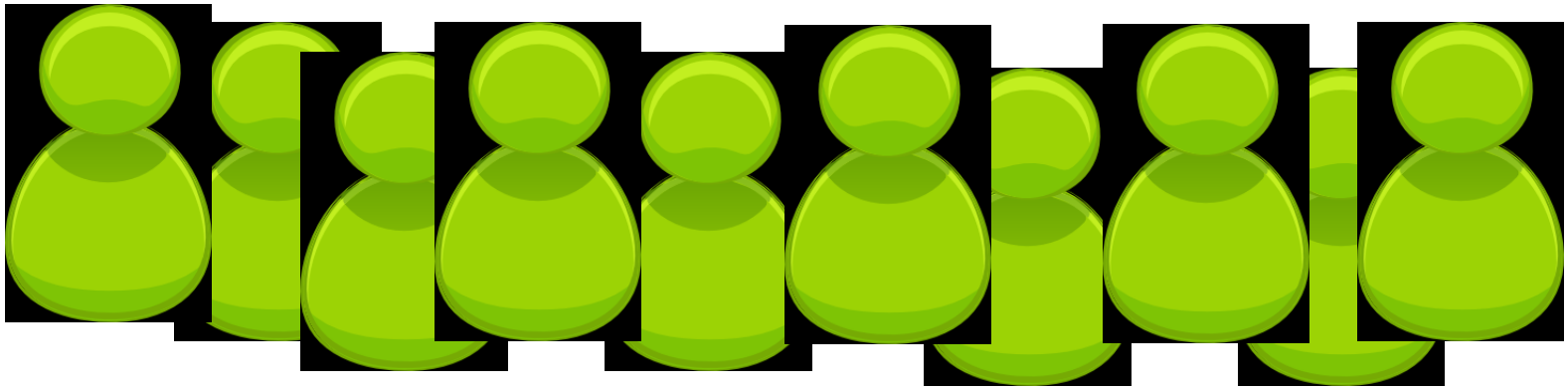
- Spaced Repetition
  - Can users recall multiple PAO stories by following spaced repetition schedules?
  - Which schedules work best?
- Mnemonic Advantage
  - Does the PAO mnemonic technique improve recall?
- Interference Effect

Outline

- Motivation
- **Study Protocol**
  - **Recruitment and Incentives**
  - Memorization Phase
  - Rehearsal Phase
  - Conditions
- Results
- Discussion
- Future Directions

Recruitment

amazon mechanical turk
Artificial Artificial Intelligence



578 participants completed initial memorization phase

User Study Protocol

- Memorization Phase (5 minutes):
  - Participants asked to memorize four randomly selected person-action object stories.
- Rehearsal Phase (120+ days):
  - Participants periodically asked to return and rehearse their stories (following rehearsal schedule)

Memorization Phase

Darth Vader

Click the image to choose a different picture

Please select a person from the drop-down list to the left to go with the scene above. Once you choose a person for this scene, you cannot change your selection. Press the Continue button when finished.

Continue

Memorization Phase

Darth Vader **bribing** **roach**

Click here to select an image for this action

Click here to select an image for this object

Your words are: bribing roach.
Imagine the person you have selected performing this action in the scene above. Type in a short story involving the person, action, and object. Make sure your words appear in your story, in the correct order. Select representative images for the actions and objects above by clicking on the placeholder images beneath the words.

Story:

Type your words twice in the boxes below.

Action	Object

Continue

Memorization Phase

Darth Vader **bribing** **roach**

Rehearsal

Please enter the pair of words that you were assigned.

Darth Vader

Select an Option

b

batting

bowing

bribing

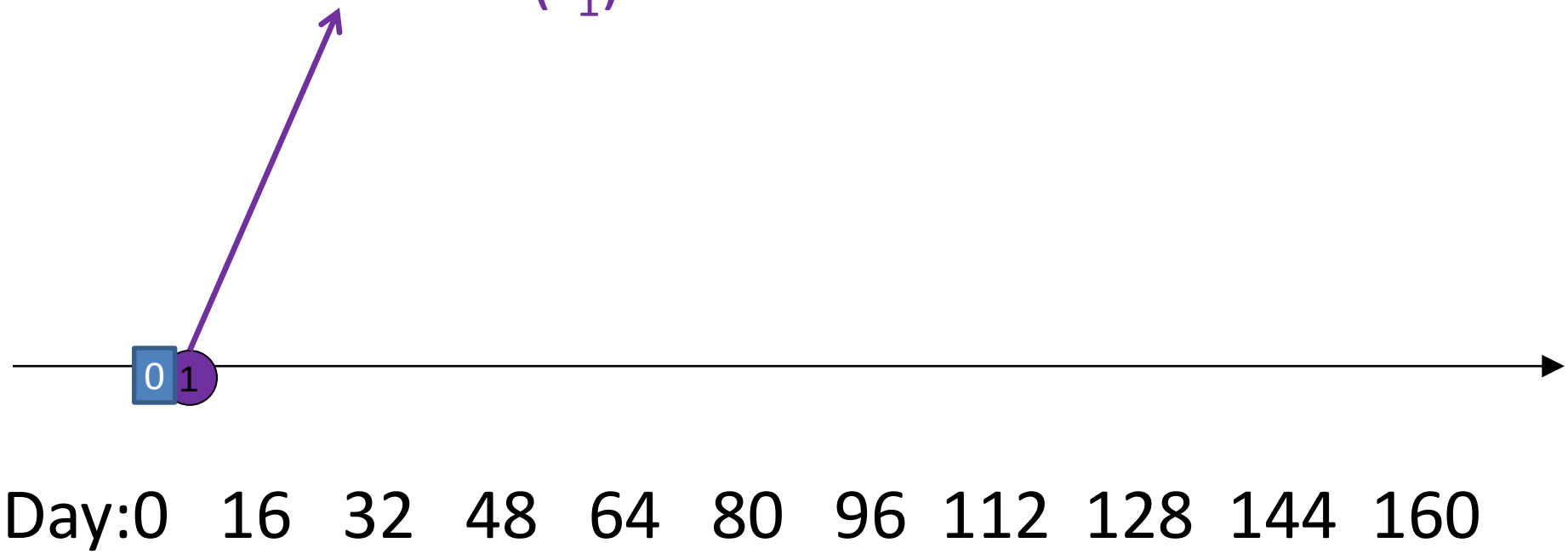
burying

Select an Option

Rehearsal Schedules

Example 1: 12hrX1.5

First Rehearsal (t_1): 12 hours

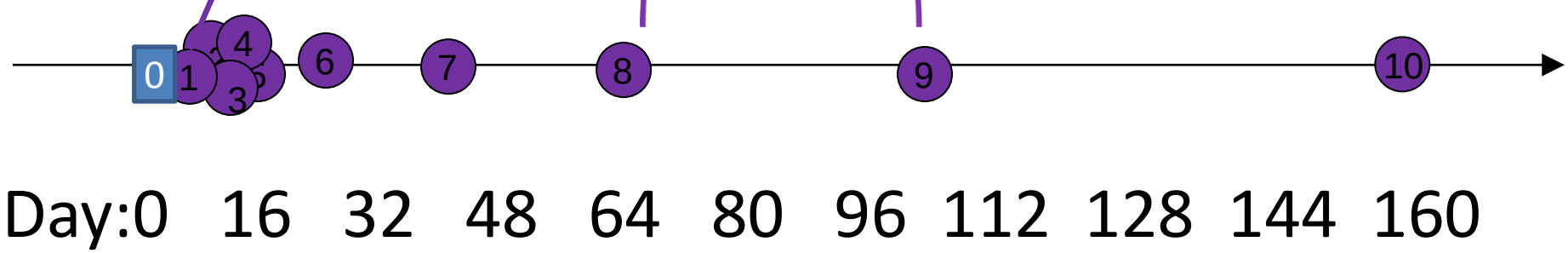


Rehearsal Schedules

Example 1: 12hrX1.5

First Rehearsal (t_1): 12 hours

$$t_{i+1} - t_i = 12hr \times (1.5)^i$$

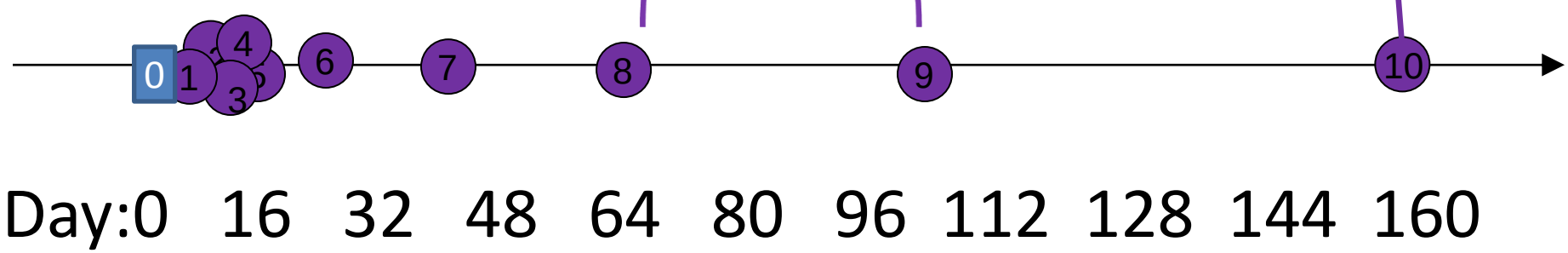


Rehearsal Schedules

Example 1: 12hrX1.5

Final Rehearsal (t_{10}): 157 days

$$t_{i+1} - t_i = 12hr \times (1.5)^i$$

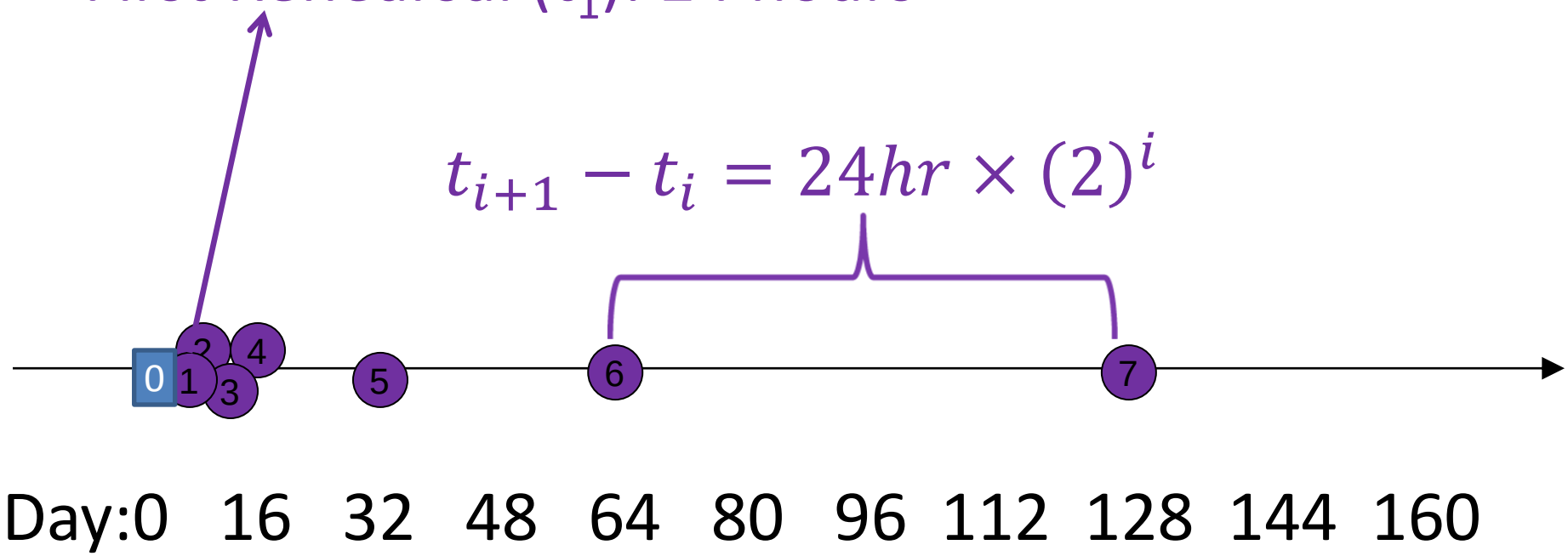


Rehearsal Schedules

Example 2: 24hrX2

First Rehearsal (t_1): 24 hours

$$t_{i+1} - t_i = 24hr \times (2)^i$$

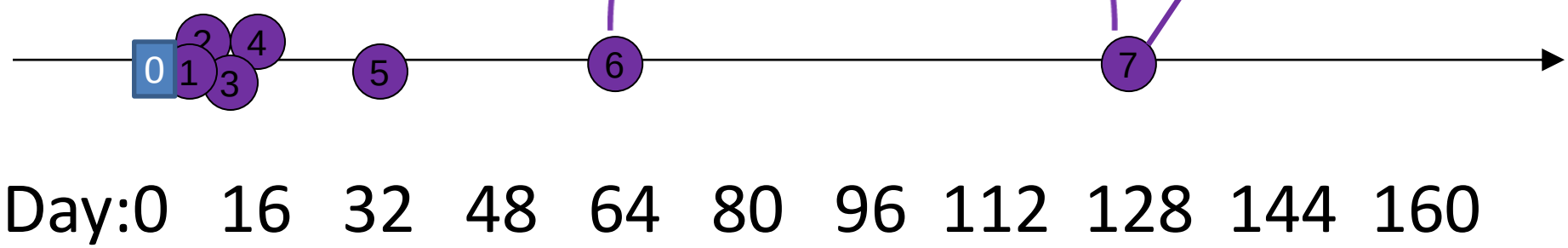


Rehearsal Schedules

Example 2: 24hrX2

Final Rehearsal (t_7): 127 days

$$t_{i+1} - t_i = 24hr \times (2)^i$$



Rehearsal Schedules

Rehearsal#/ Schedule	1	2	3	4	5	6	7	8	9	10	11	12
12hrx1.5	.5 day	1.75	4.2	8.2	14.7	24.7	40.7	64.7	101.7	157.7	N/A	N/A
24hrX2	1 day	3	7	15	31	63	127	N/A	N/A	N/A	N/A	N/A
24hrX2+2Start	.1 day	.6	1.6	3.6	7.6	15.6	31.6	63.6	127.6	N/A	N/A	N/A
30minX2	.5 hr	1.5hr	3.5 hr	7.5 hr	15.5 hr	1.7 day	3.7	7.7	15.7	31.7	63.7	127.7

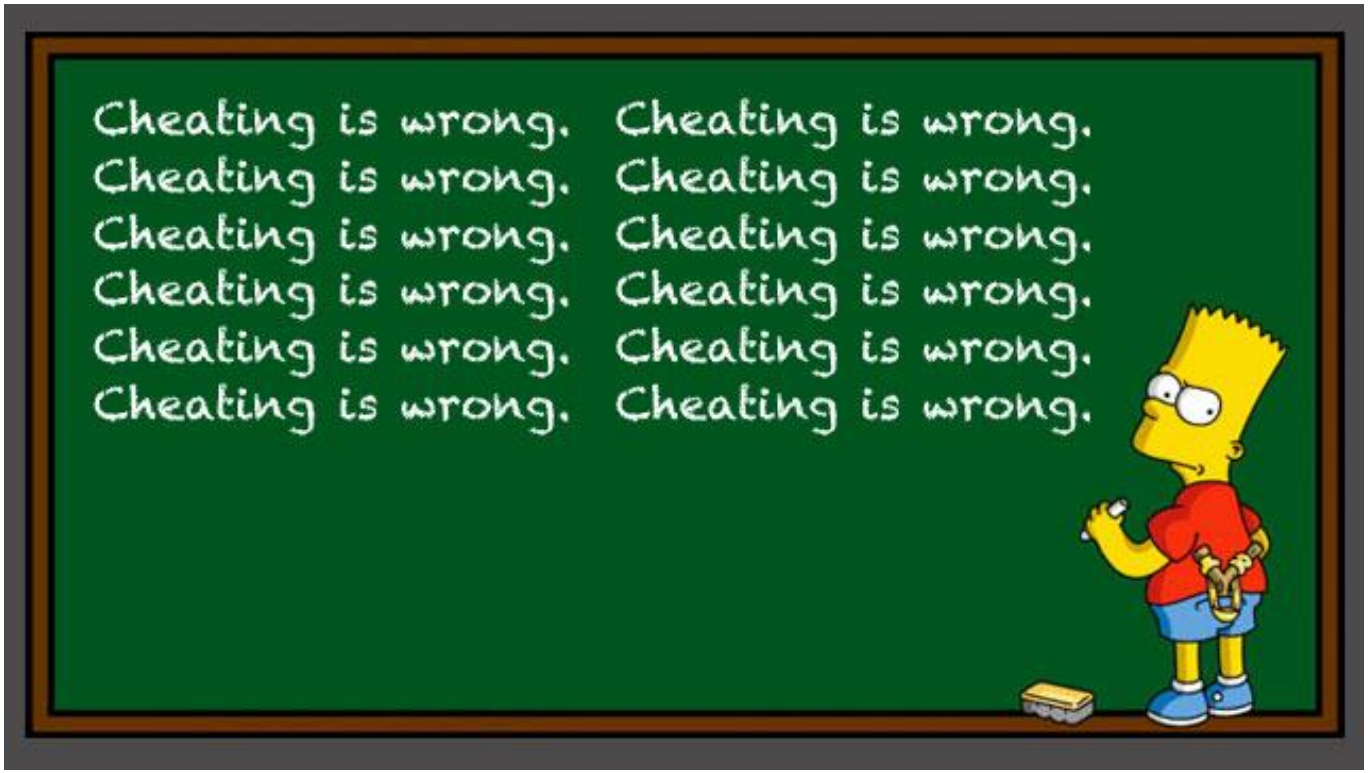
Incentives

- Memorization Phase ($0.5)

- Rehearsal Phase ($0.75 each)
  - Encourage participants to return
  - Discourage Cheating

Do Not Write Down Your Words

- "…we ask that you do not write down the words that we ask you to memorize."



Do Not Write Down Your Words

- "…we ask that you do not write down the words that we ask you to memorize."
- "You will be paid for each completed rehearsal phase --- even if you forgot the words."
- "**Important:** …do not write down the words"
- "You will be paid for each completed rehearsal phase --- even if you forgot the words."

Study Conditions

- **Mnemonic/text**
- **Rehearsal Schedule**
- **# PAO Stories**
  - **One, Two or Four**

m_12hrX1.5_4

Study Conditions

Condition	Comment
m_24hrX2+2Start_1	1 PAO Story
m_24hrX2+2Start_2	2 PAO Stories
m_24hrX2+2Start_4	4 PAO Stories

Interference

Condition	Comment
t_24hrX2+2Start_4	Text condition/No Cues
m_24hrX2+2Start_4	Mnemonic Condition

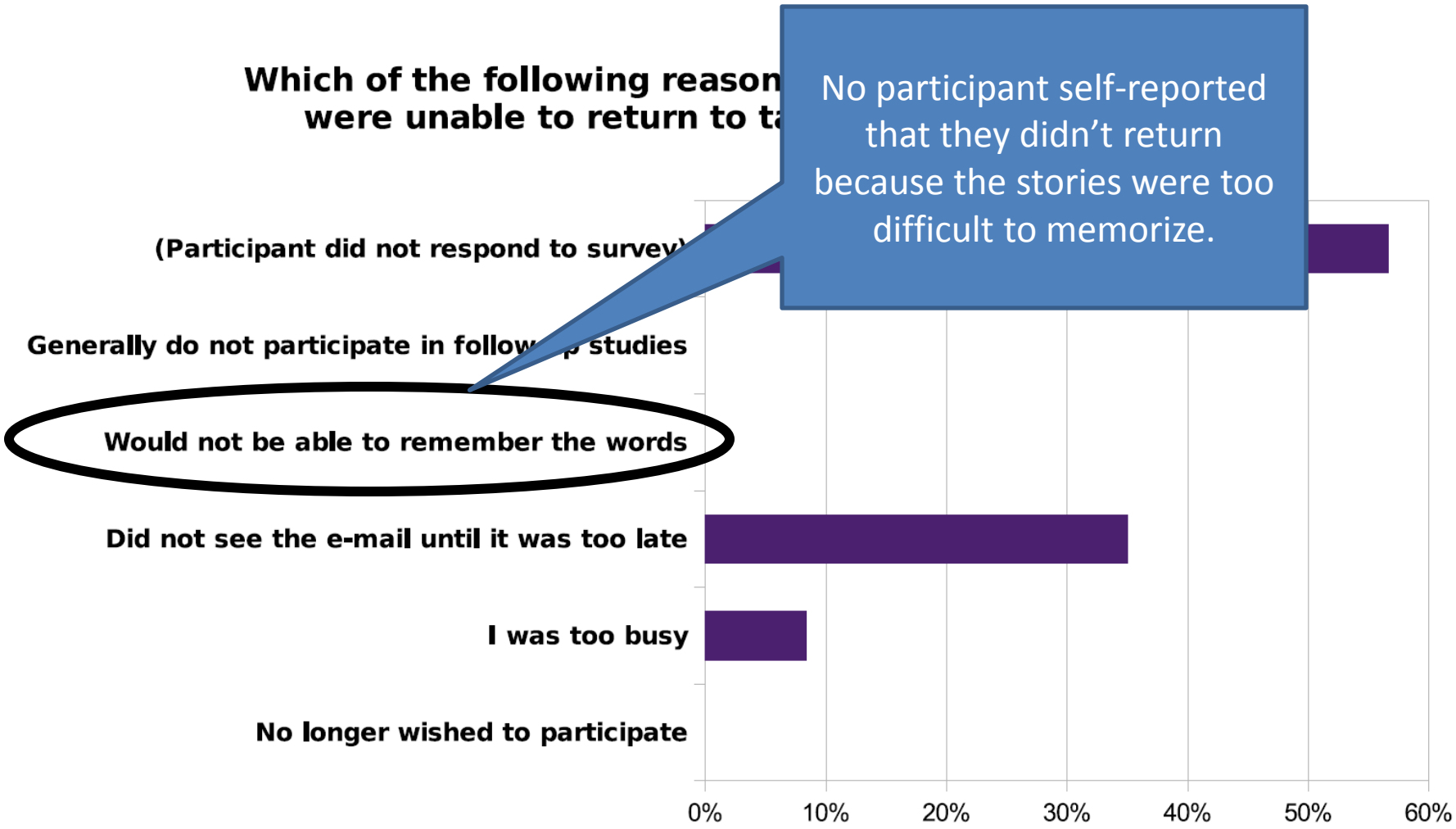
Mnemonic vs Text

Study Conditions

Condition	Comment
m_24hrX2_4	24 hour base
m_24hrX2+2Start_4	Two Extra Rehearsals on Day 1
m_30minX2_4	30 min base
m_12hrX1.5_4	Growth Rate: 1.5x

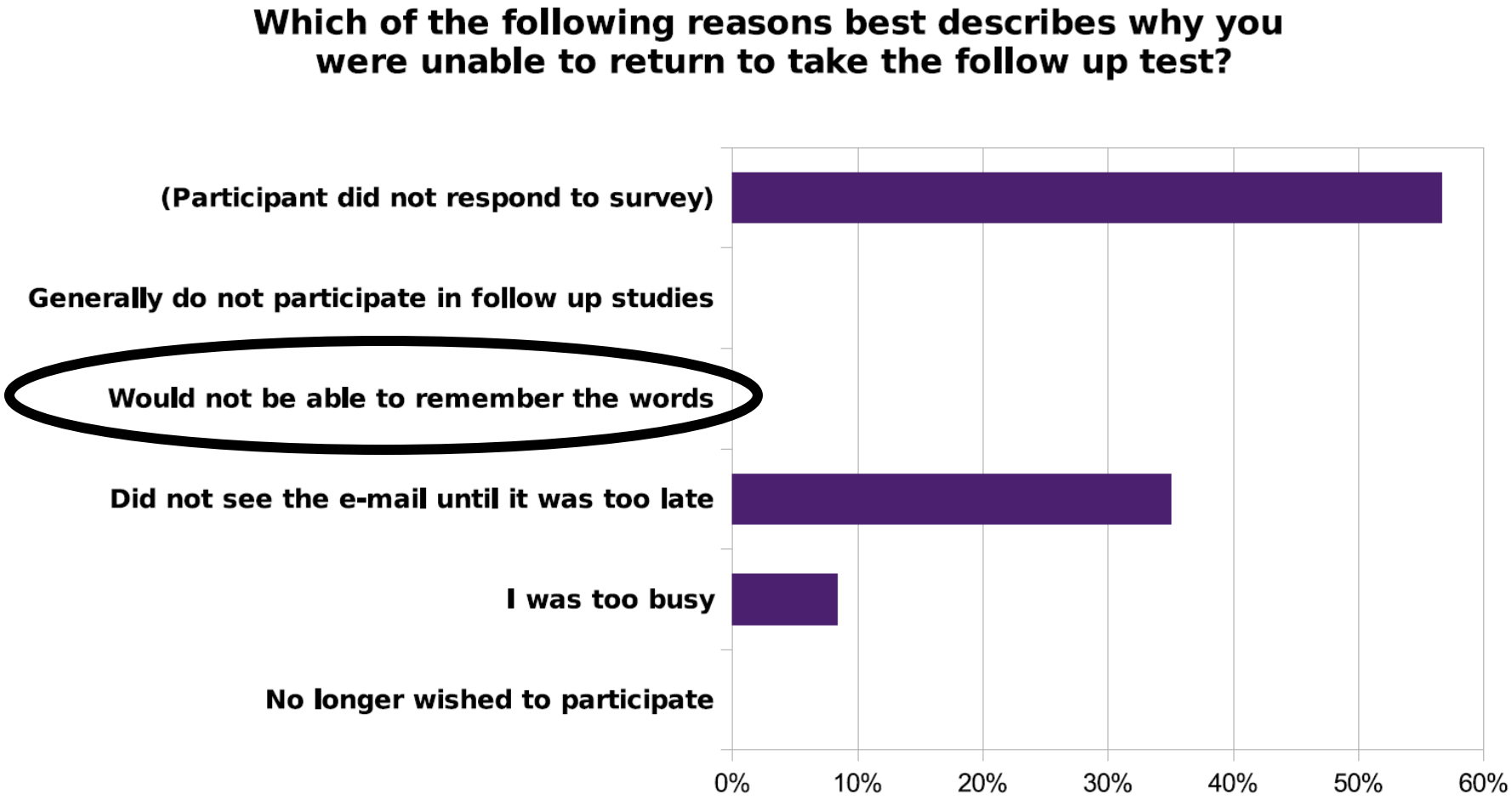
Compare Rehearsal Schedules

Survey: Dropped Participants



No participant self-reported that they didn't return because the stories were too difficult to memorize.

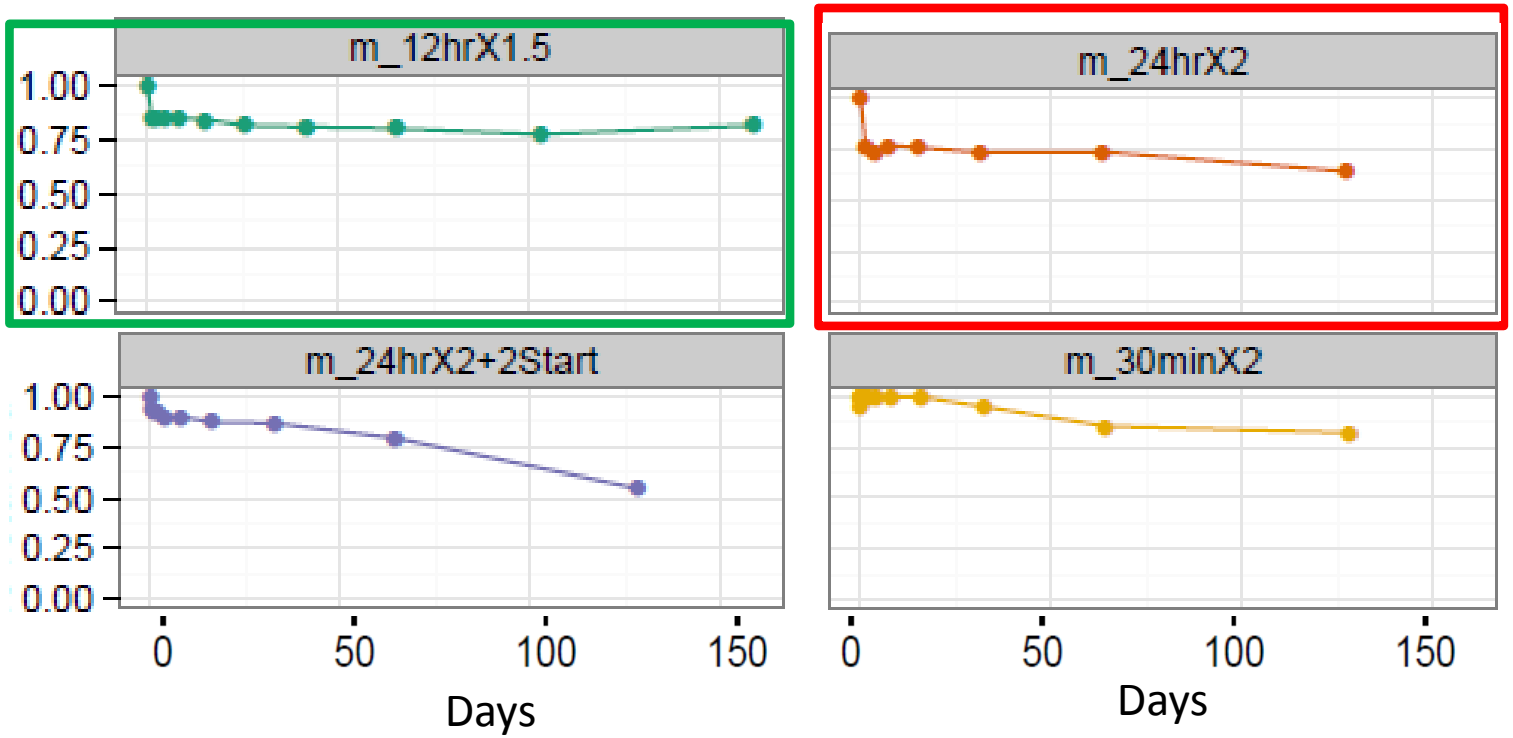
Survey: Dropped Participants



Outline

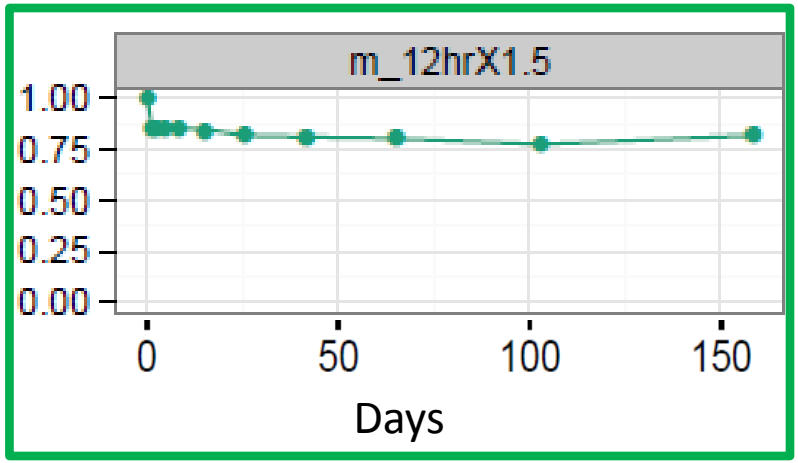
- Motivation
- Study Protocol
- **Results**
- Discussion
- Future Directions

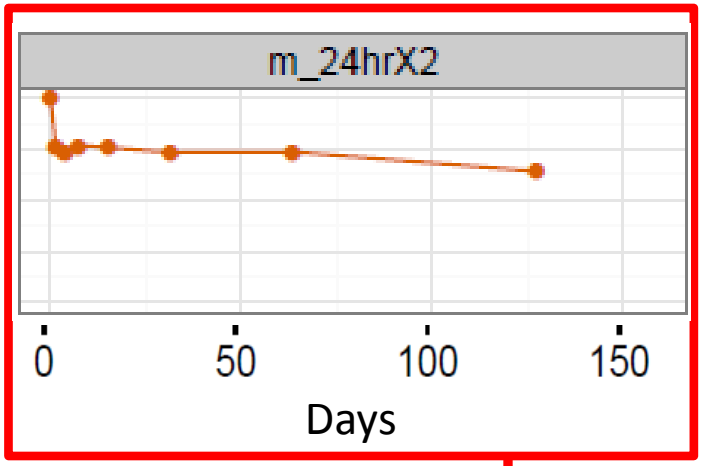
Rehearsal Schedules



Survived(i)/Returned(i)

Rehearsal Schedules





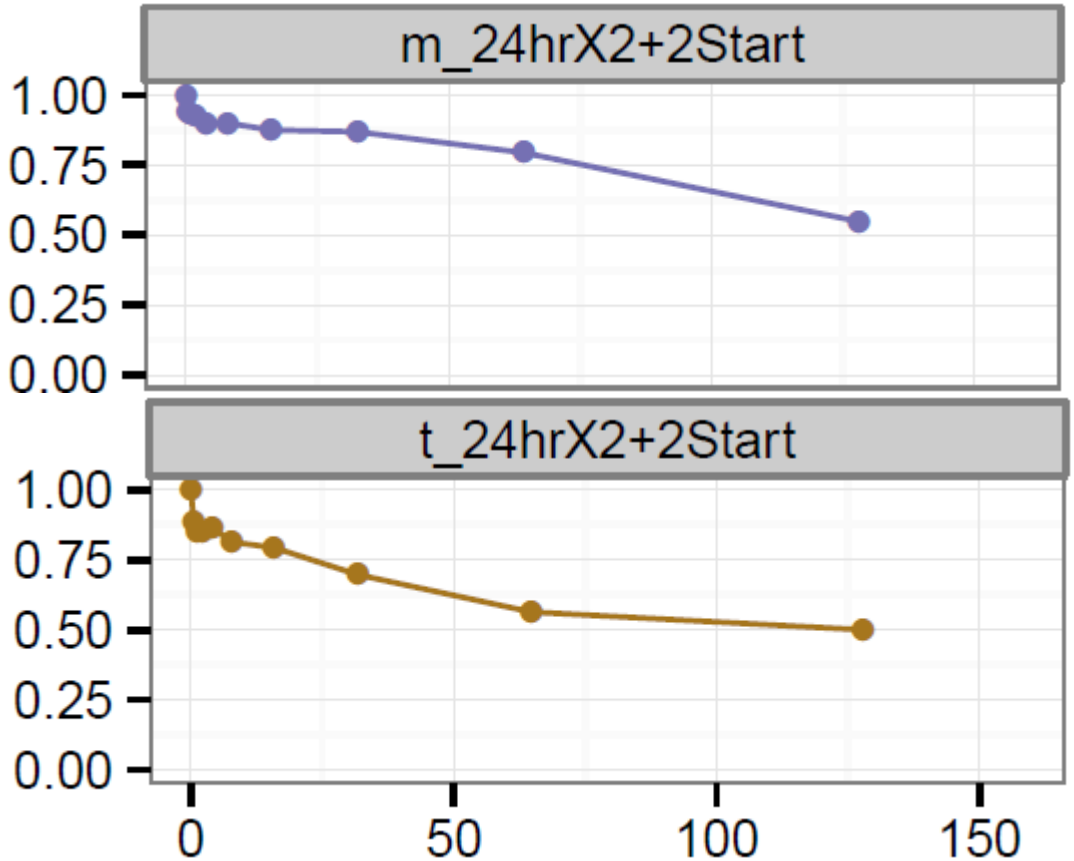
Survived(i)/Returned(i)

$$\mathrm{Exp}(\beta) = 0.42\ *$$

Participants twice as likely to fail at any given point in time

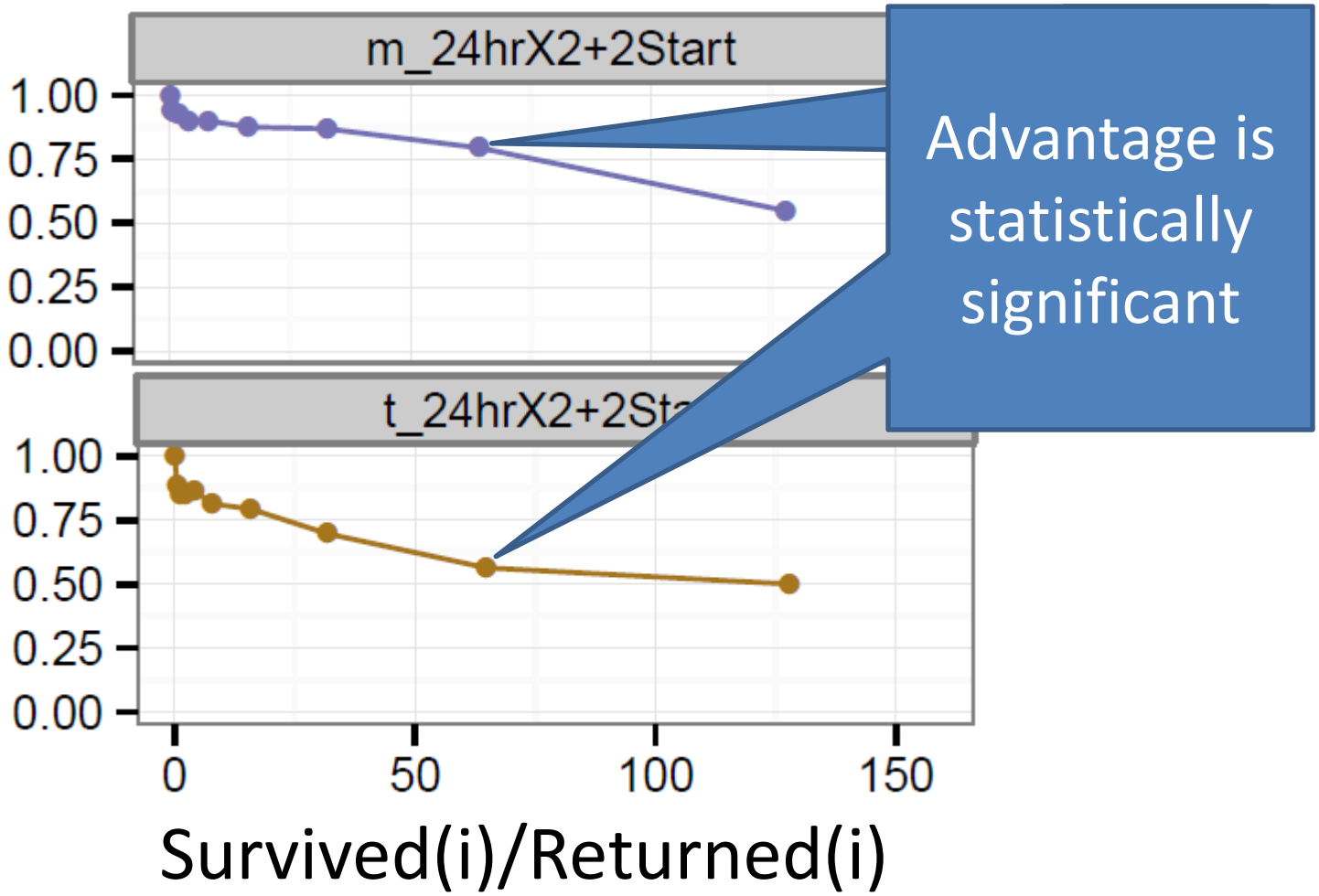
*** Statistically Significant (p=0.05)**

Text vs Mnemonic

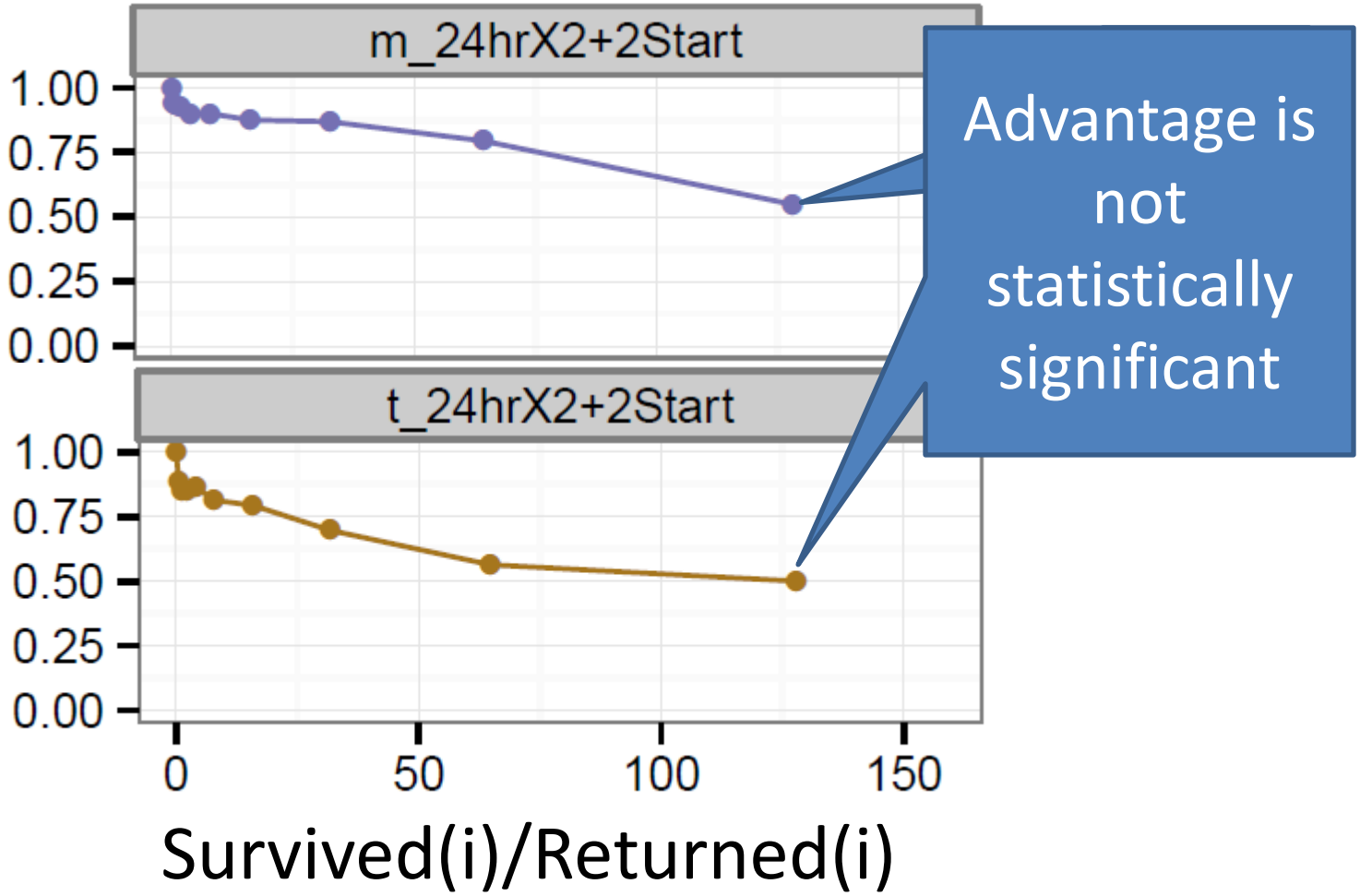


Survived(i)/Returned(i)

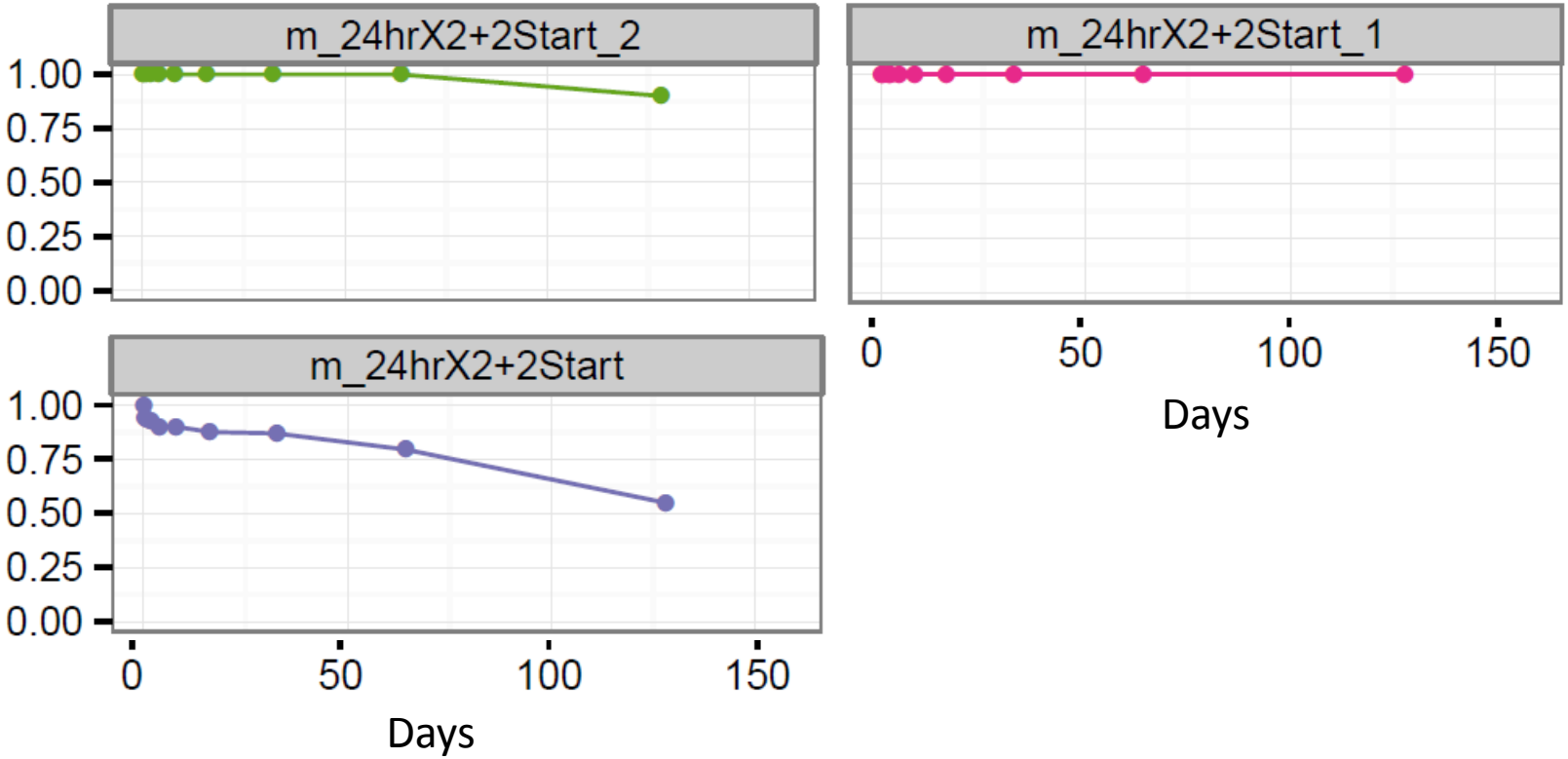
Text vs Mnemonic



Text vs Mnemonic



Interference



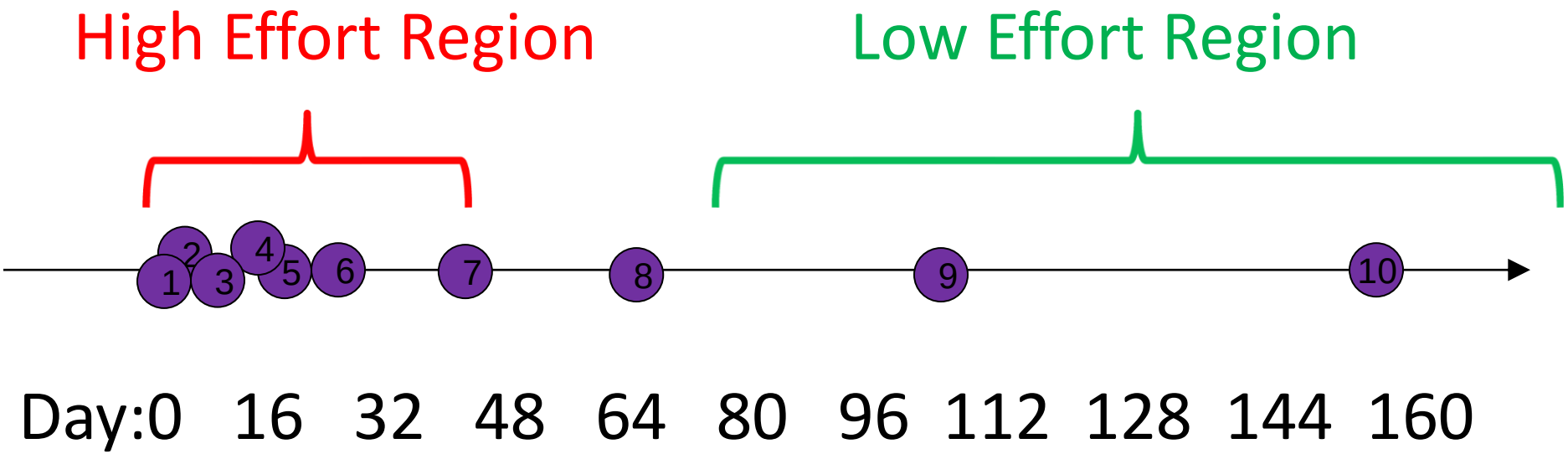
Survived(i)/Returned(i)

Interference Effect was Statistically Significant

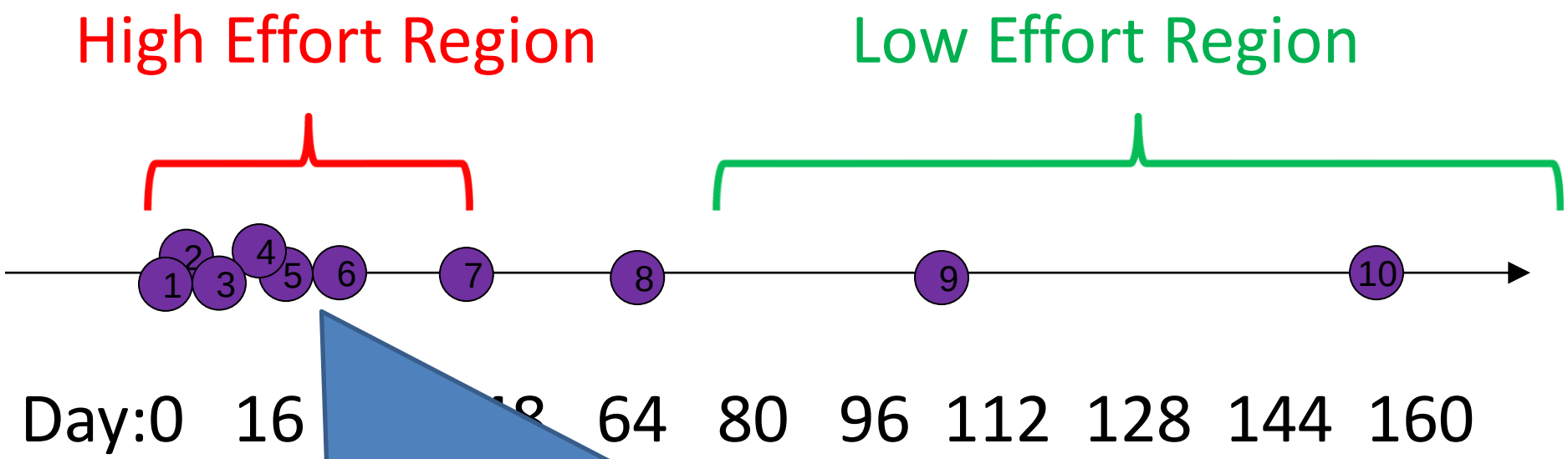
Outline

- Motivation
- Study Protocol
- Results
- **Discussion & Future Directions**
  - Password Expiration Policies
  - Password Strengthening
  - Mitigating Interference

Our Take: Password Expiration Policies



Our Take: Password Expiration Policies



We believe our study calls into question the merit of continuing the practice of password expiration.

The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis

Yinqian Zhang
University of North Carolina at Chapel Hill
Chapel Hill, NC
yinqian@cs.unc.edu

Fabian Monrose
University of North Carolina at Chapel Hill
Chapel Hill, NC
fabian@cs.unc.edu

Michael K. Reiter
University of North Carolina at Chapel Hill
Chapel Hill, NC
reiter@cs.unc.edu

ABSTRACT

This paper presents the first large-scale study of the success of password expiration in meeting its intended purpose, namely revoking access to an account by an attacker who has captured the account's password. Using a dataset of over 7700 accounts, we assess the extent to which passwords that users choose to replace expired ones pose an obstacle to the attacker's continued access. We develop a framework by which an attacker can search for a user's new password from an old one, and design an efficient algorithm to build an approximately optimal search strategy. We then use this strategy to measure the difficulty of breaking newly chosen passwords from old ones. We believe our study calls into question the merit of continuing the practice of password expiration.

> *an attacker wants to do all of the damage that he's going to do right now. It does offer a benefit when the attacker intends to continue accessing a system for an extended period of time.* [2]

At this level of specificity, such an argument is unquestionably sound. However, the process of reducing such intuition to a reasonable password expiration policy would ideally be grounded in measurements of what "additional steps" the policy hoists on an attacker, so as to be certain that these "additional steps" are an impediment to his continued access. Unfortunately, even to this day, the security community has yet to provide any such measurements.

In this paper we provide the first analysis of which we are aware of the effectiveness of expiring passwords. Using a dataset of pass-

The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis

Yinqian Zhang
University of North Carolina at Chapel Hill
Chapel Hill, NC
yinqian@cs.unc.edu

Fabian Monrose
University of North Carolina at Chapel Hill
Chapel Hill, NC
fabian@cs.unc.edu

Michael K. Reiter
University of North Carolina at Chapel Hill
Chapel Hill, NC
reiter@cs.unc.edu

ABSTRACT

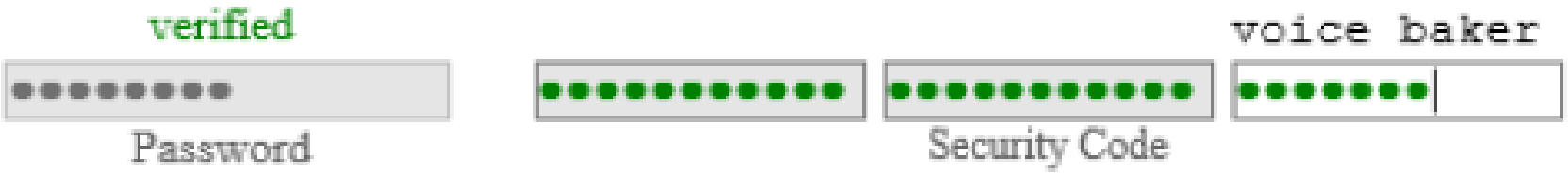
This paper presents the first large-scale study of the success of password expiration in meeting its intended purpose, namely revoking access to an account by an attacker who has captured the account's password. Using a dataset of over 7700 accounts, we assess the extent to which passwords that users choose to replace expired ones pose an obstacle to the attacker's continued access. We develop a framework by which an attacker can search for a user's new password from an old one, and design an efficient algorithm to build an approximately optimal search strategy. We then use this strat-

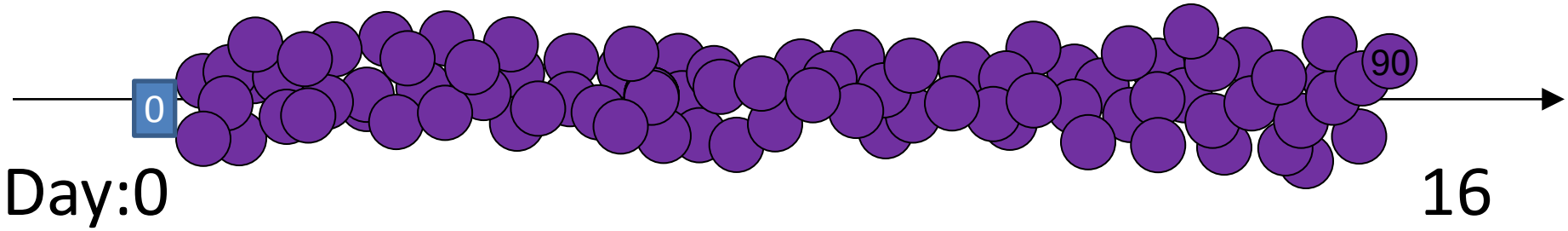
from old ones. We believe our study calls into question the merit of continuing the practice of password expiration.

We believe our study calls into question the merit of continuing the practice of password expiration.

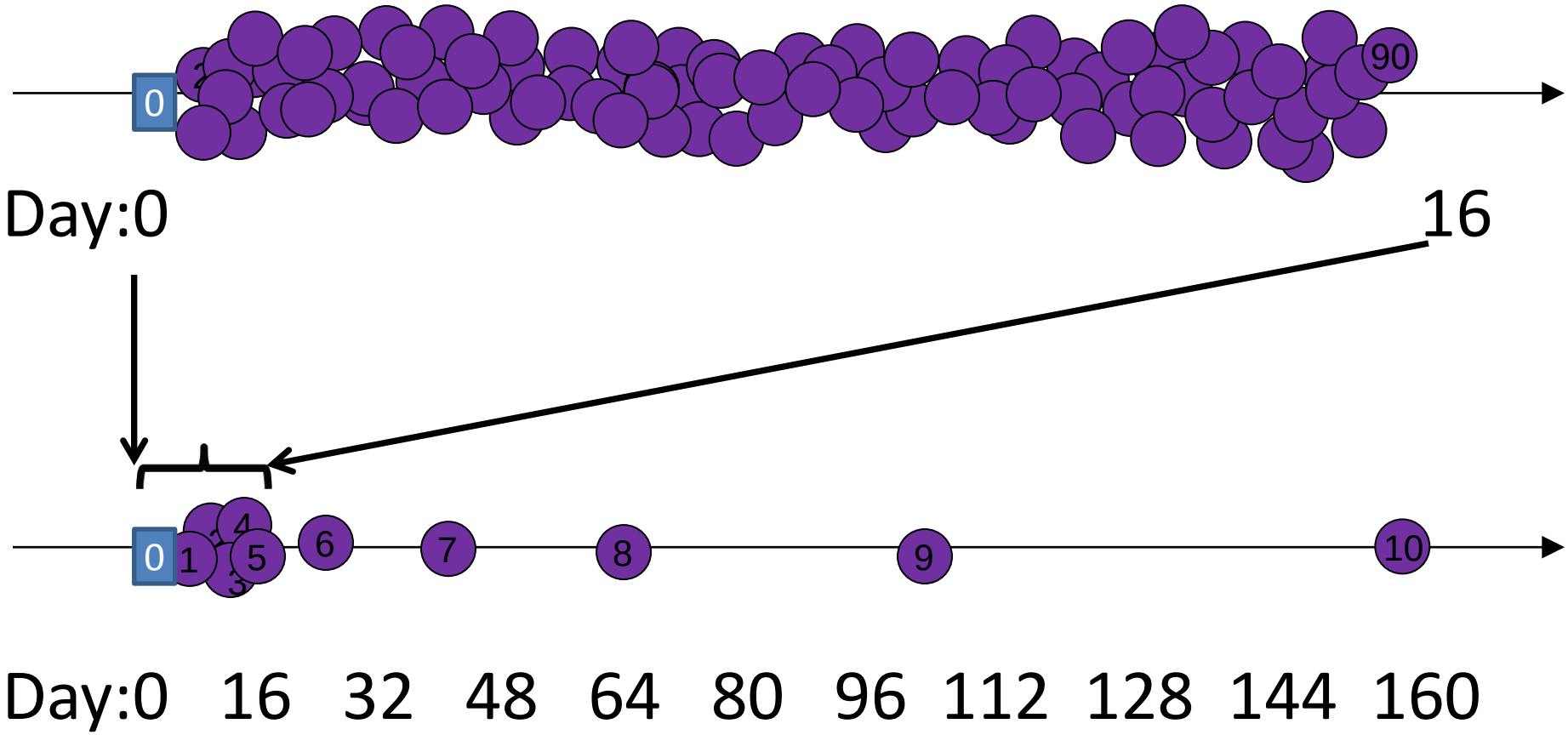
Password Strengthening

- Towards reliable storage of 56-bit secrets in human memory [BS14]





Related Work

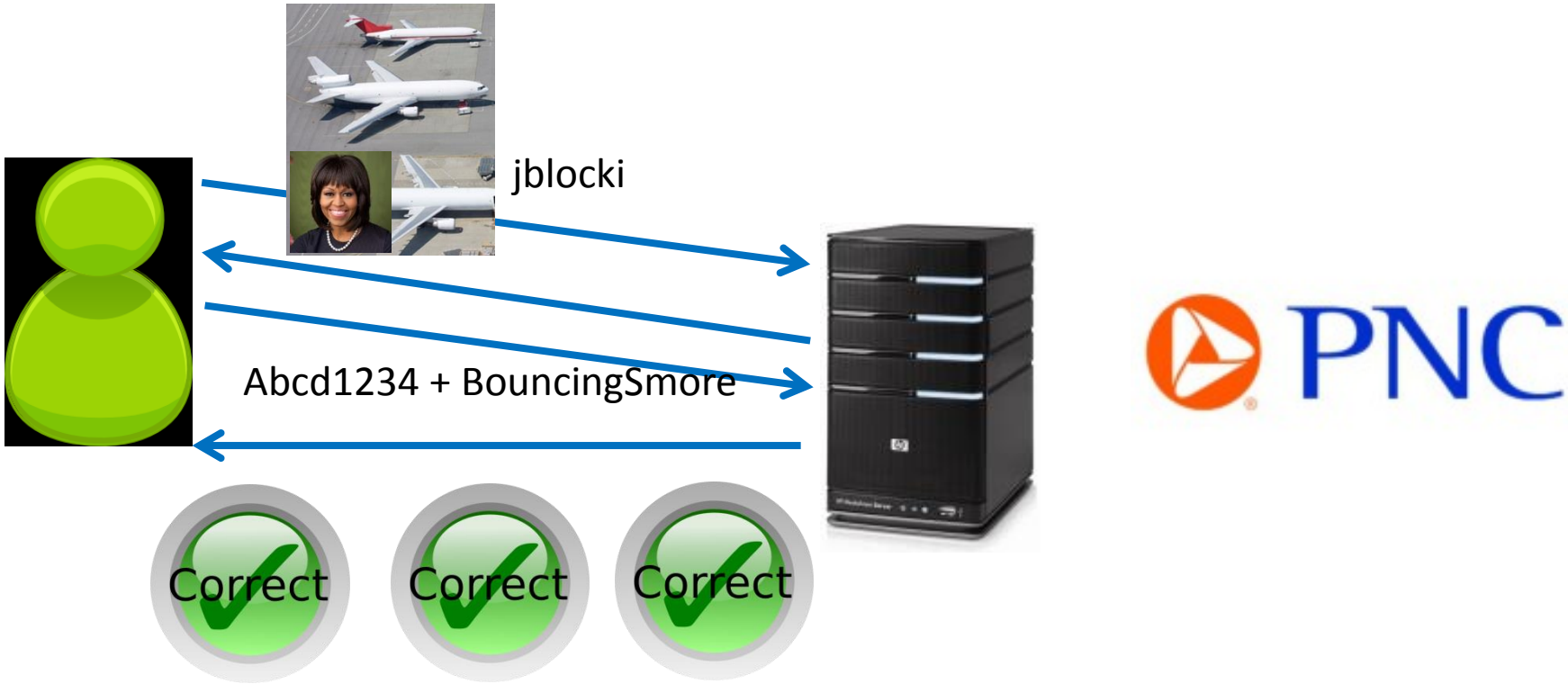


Password Strengthening Mechanism

Password Strengthening Mechanism

Password Strengthening Mechanism

Password Strengthening Mechanism



Once we can be confident that the user will remember the story we add it to the password.

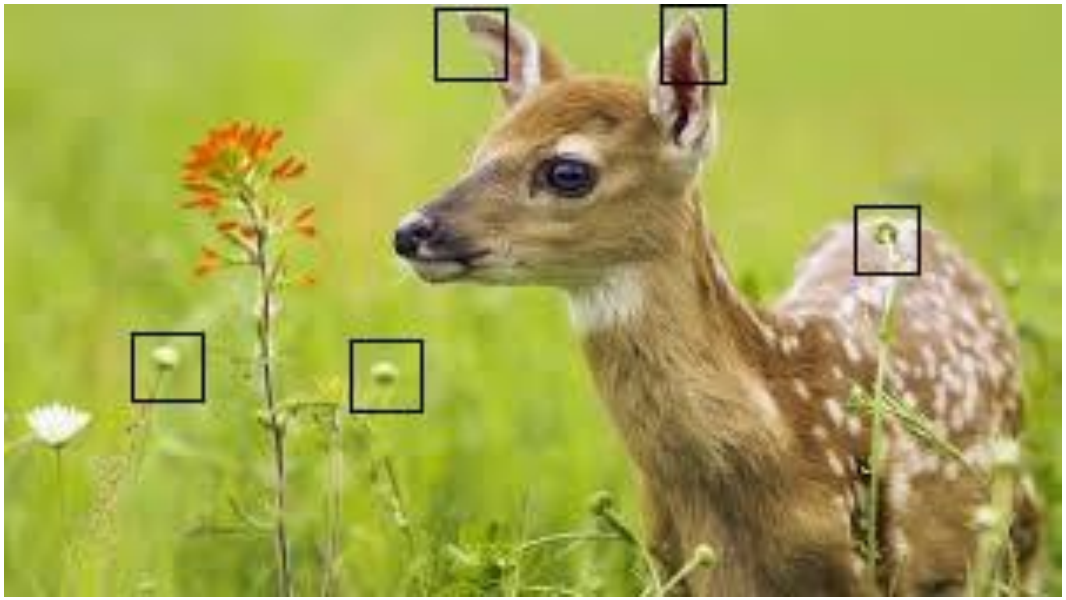
Future Directions

- Understand the Cause(s) of Interference
  - User Fatigue?
  - Mixing up stories?

- Mitigating Interference
  - Staggered Memorization Schedule?
  - Gracefully Expanding Combinatorial Designs

Future Directions

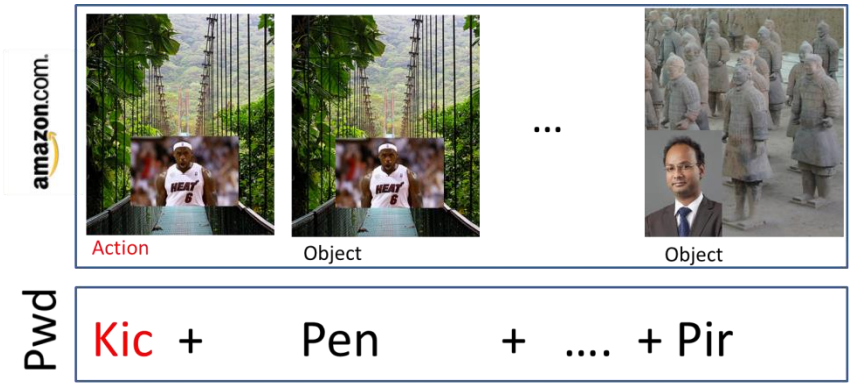
- Spaced Repetition with other mnemonics
  - Graphical Secrets

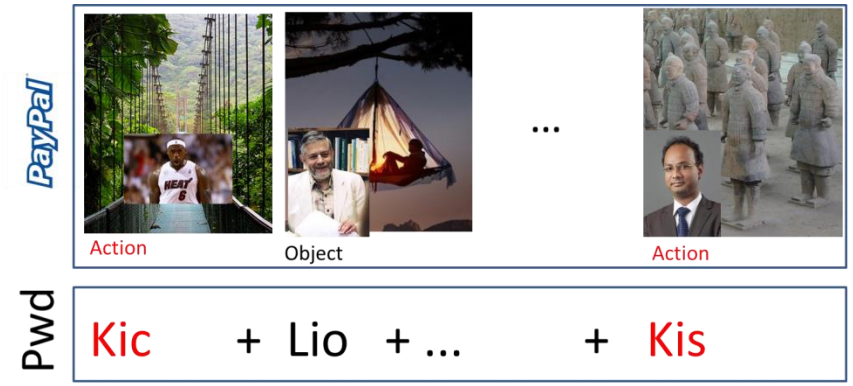


Thanks for Listening

Conclusion

Spaced Repetition and Mnemonics Enable Recall of Multiple Strong Passwords





⋮ ⋮

Related Work

- Password Management Software

LastPass ****
The Last Password You'll Ever Need.

Related Work

Goal: Minimize Trust Assumptions about User's Computational Devices

Related Work

- Alternatives to Passwords

OpenID®

Related Work

Quest to Replace Passwords [BHOS2012]