

# Password Management Strategies for Online Accounts

Shirley Gaw, Edward W. Felten  
Princeton University

## Abstract

Average number of **unique passwords**  
3.31 (n = 49, SD = 1.76)  
...and average **reuse**  
3.18 (SD = 2.71)

People will **reuse** passwords more as they acquire more accounts

## Abstract (continued)

Why reuse?

The reused ones were easier to remember

People rely on their **memory** rather than store passwords

## Abstract (continued)

Friends have the greatest **ability** to attack passwords

Participants ranked those **closest** to them as having the greatest **ability** to compromise their passwords

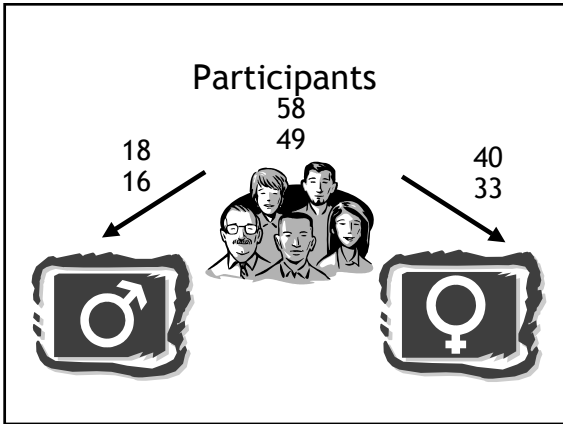
## Abstract (continued)

Knowing personal information about a victim was seen as advantageous

People worry more about **human** guessing than **automated** guessing tools

## Outline

People will **reuse** passwords more as they acquire more accounts  
People rely on their **memory** rather than store passwords  
Reasons for Reuse  
Participants ranked those **closest** to them as having the greatest **ability** to compromise their passwords  
Perceptions of Attacks  
People worry more about **human** guessing than **automated** guessing tools



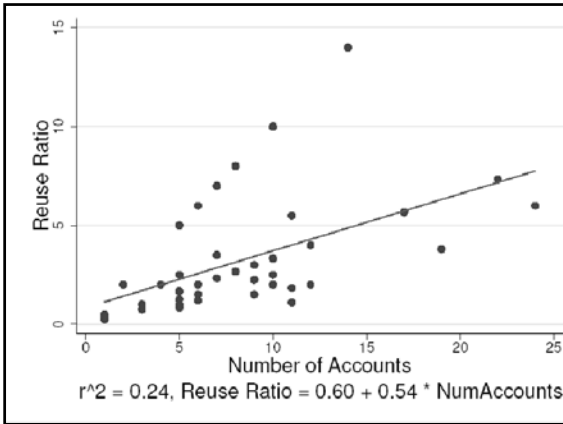
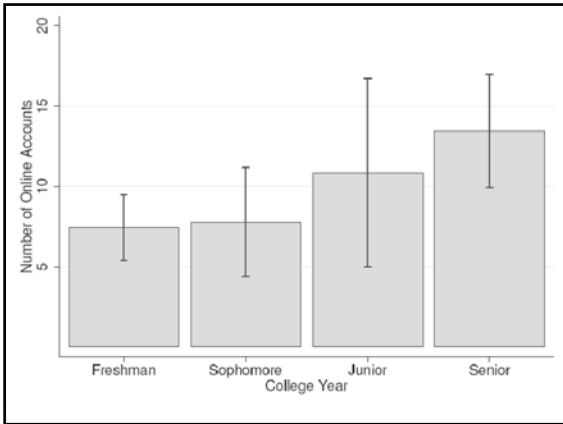
- ### Outline
- Password Reuse
  - Reasons for Reuse
  - Perceptions of Attackers
  - Perceptions of Attack

- ### Password Reuse: Method
- First Pass:* (n = 49)
- Select from 139 websites
  - Login to each website
  - Self-report summary statistics
- Second Pass:*
- List other websites used personally
  - Re-report summary statistics

### Password Reuse: Results

Unique passwords  
M = 3.31, SD = 1.76 (n = 49)

Passwords reuse rate  
M = 3.18, SD = 2.71



## Password Reuse: Results

People will **reuse** passwords more as they acquire more accounts

## Outline

- Password Reuse
- **Reasons for Reuse**
- Perceptions of Attackers
- Perceptions of Attack

## Reasons for Reuse: Method

115 question survey (n = 58)

- Demographic information
- Explanations of password reuse/avoidance
- Descriptions of password creation/storage
- Descriptions of password management

## Reasons for Reuse: Results

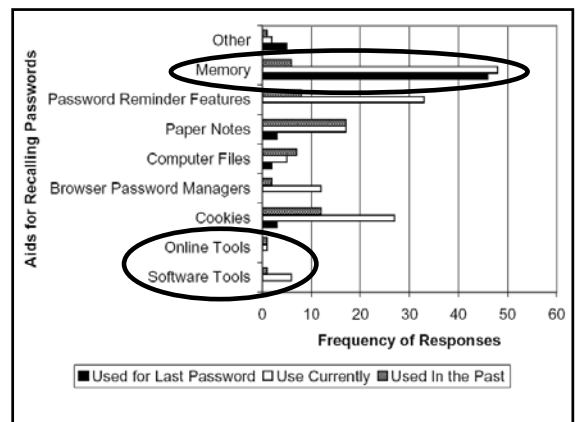
Why use a different password?

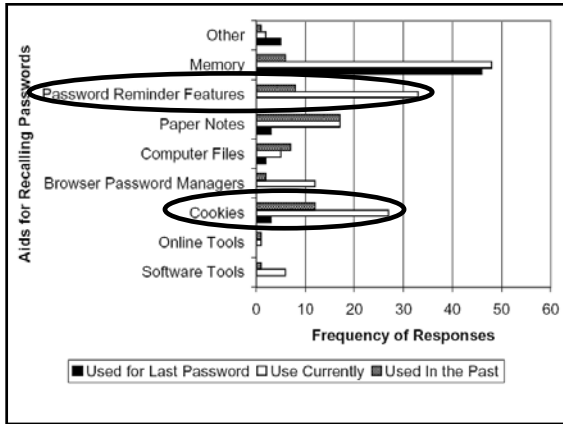
- Security (12)
- Website has credit card, etc (11)
- Website restricts password format (10)
- Website is important (7)
- Website is in a particular category (4)
- Other (12)

## Reasons for Reuse: Results

Why use the same password?

It is easier to **remember** (35)





### Reasons for Reuse: Results

Why use the same password?  
It is easier to **remember** (35)

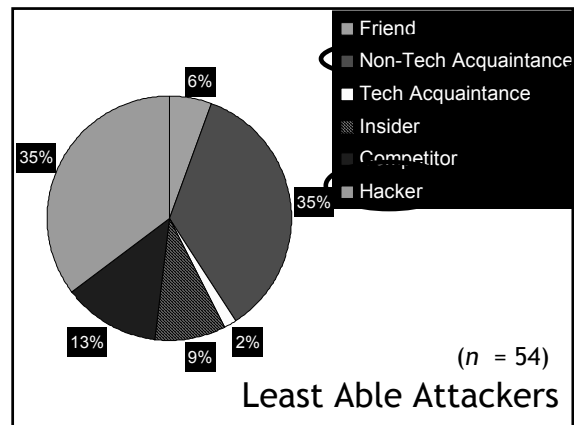
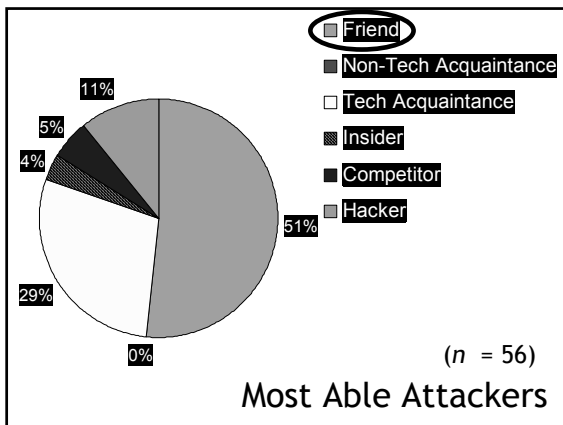
People rely on their **memory** rather than store passwords

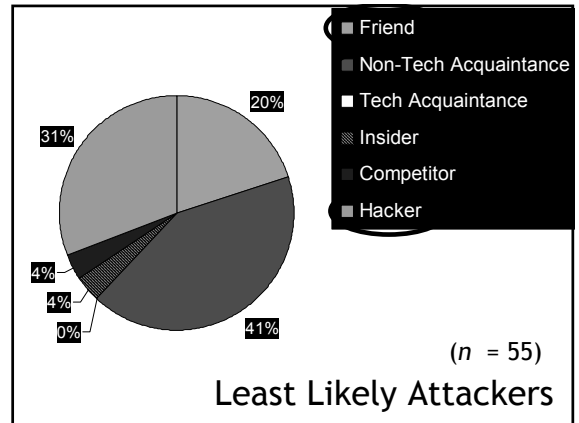
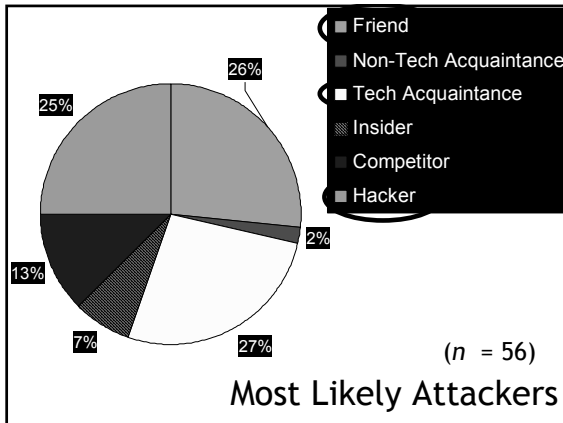
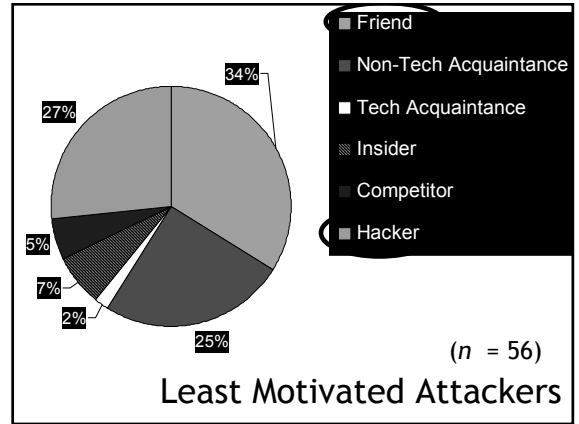
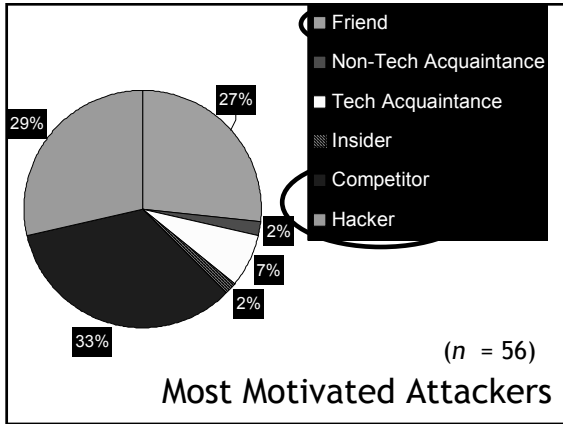
### Outline

- Password Reuse
- Reasons for Reuse
- **Perceptions of Attackers**
- Perceptions of Attack

### Perceptions of Attackers: Method

- Who could compromise password? Rank
  - Ability (n = 56)
  - Motivation
  - Likelihood
- Categories of people
  - Friend
  - Acquaintance (tech & non-tech)
  - Competitor
  - Insider
  - Hacker





### Likely attackers: Motivated or Able?

- Logit regression on ranking responses\*
- Odds on ranking someone as likely
  - Motivation: 6.28 x
  - Ability: 3.82 x

\*Thanks to Pierre-Antoine Kremp

### Perceptions of Attackers: Results

Participants ranked those **closest** to them as having the greatest **ability** to compromise their passwords

## Outline

- Password Reuse
- Reasons for Reuse
- Perceptions of Attackers
- **Perceptions of Attack**

## Perceptions of Attacks: Method

*Given:* (n = 56)

13 tips for creating strong passwords

- 3 passwords
- Password construction method

*Task:*

- Rank passwords by strength
- Explain ranking

## Perceptions of Attacks: Results

*PrincetonNJ is too easy for someone to guess if they **know where you live***

*One would **have to know her** decently well to know her favorite novel*

## Perceptions of Attacks: Results

People worry more about **human** guessing than **automated** guessing tools

## Good News / Bad News

- Good news: Participants understood the threat posed by those closest to them
- Bad news: They didn't understand the threat of dictionary attacks

## Good News / Bad News

- Good news: Participants were concerned about the weakness of poor passwords
- Good news: They relied on their memory rather than poorly secured storage (ie., paper)
- Bad news: They feel and act as if they do not have any better tools or strategies

## Good News / Bad News

- Good news: Participants had few accounts with password authentication
- Bad news: They had even fewer passwords

## Outline

- Password Reuse
- Reasons for Reuse
- Perceptions of Attackers
- Perceptions of Attack