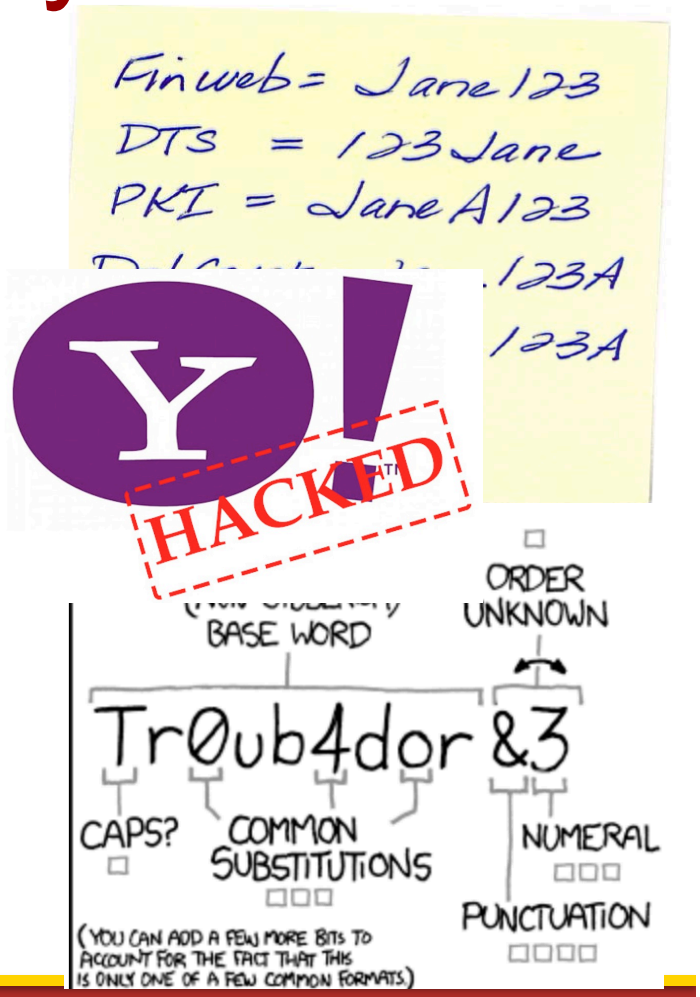
Password Research at STEEL Group

Jelena Mirkovic

Information Sciences Institute (ISI)
Marina Del Rey

Passwords: Necessary and Bad

- Everyone uses passwords
- Many problems:
  - Memorable passwords are easily cracked
  - Secure passwords hard to remember
  - Similar/same passwords are used for multiple accounts



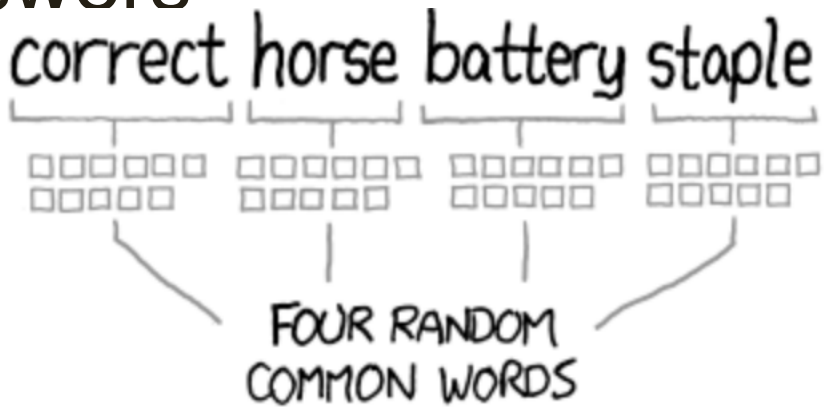
Security Qs And Passphrases

Security Questions

- Not generally applicable
- Memorable but easily guessed
- People provide fake answers

Passphrases

- Longer than passwords
- Predictable



Three Select Projects

- ***Life-Experience Passwords:*** How to use existing memories to build a new type of passwords
- ***MNPass:*** How to use mnemonics to improve passphrases
- ***SemTrac:*** How people reuse passwords

Life-Experience Passwords (LEPs)

with Simon Woo (USC CS), Elsi Kaiser (USC Psycholinguistics), Ron Artstein (ICT NLP)

Motivation of LEPs

- Users create passwords based on facts they remember about past events from their life (no burden on memory)
- Relying on existing events makes LEPs
  - Memorable (no new memories)
  - Unique (each person is different)
  - Less reused (abundance of memories to choose from)

Example

Title: My wedding

Which city did you get married in: Paris

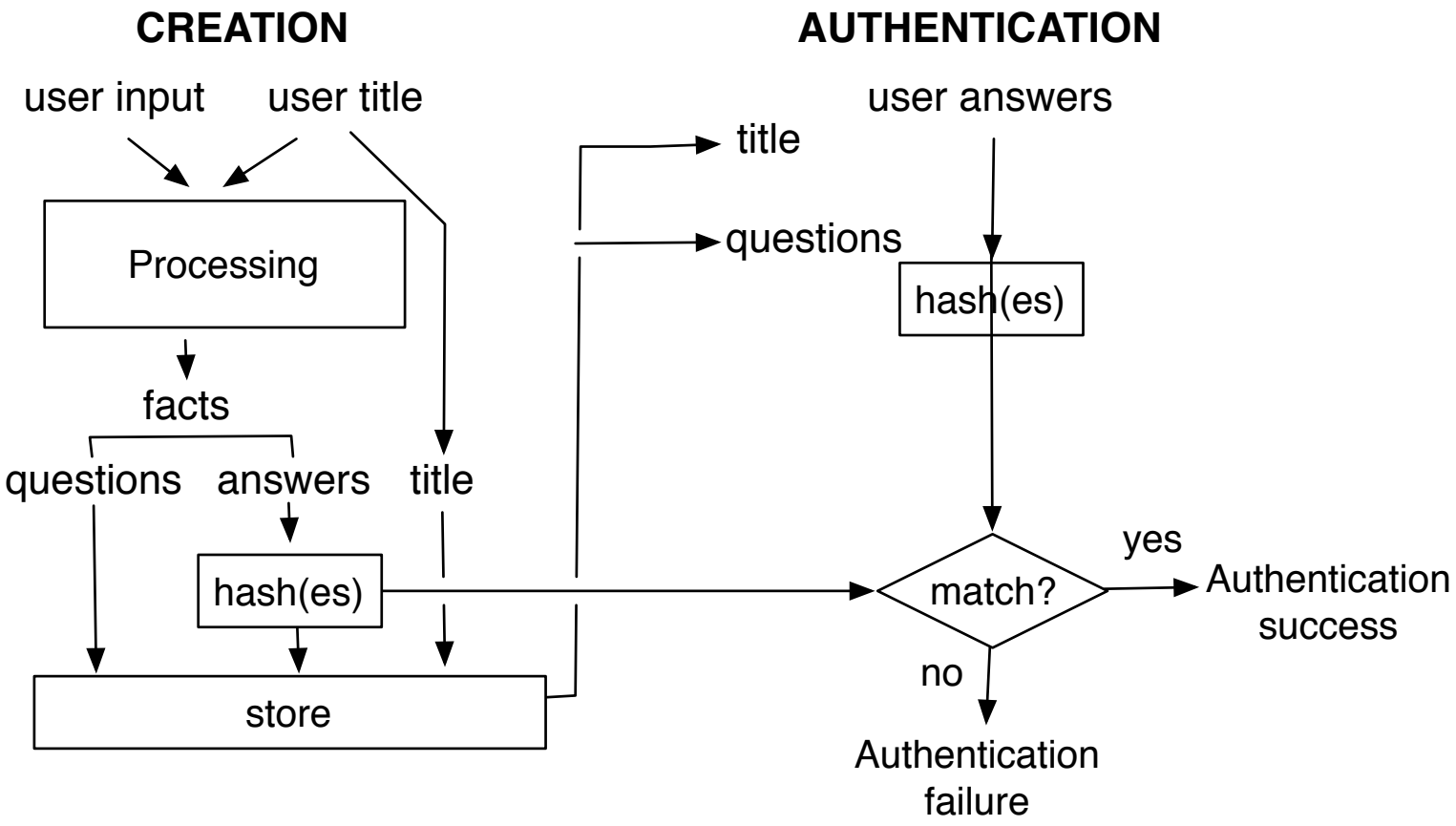
Who did your makeup: Samantha Cox

Who brought chocolate cake: Jillian Grey

What did your mom bring as a gift: red scarf

What kind of ring you got: orange diamond

How LEPs work ?



LEP Design

- **Topics:** engagement, wedding, birth, death, accident, graduation, party, trip, learning a skill or language, person, place
- **Useful facts:** strong, stable and immutable
  - People, locations, time, objects, activities
  - Elicitation specificity matters
  - Need relaxed matching
- **Sensitive facts:** 3% of users in our study, can be minimized through better elicitation

Two Elicitation Methods

User Input

Title: Trip to France
How many memorable cities did you visit? 2
List two memorable cities you visited? Paris, Nice
When did you travel? 2015
How many people traveled with you? 1
List the first and last name of the person that traveled with you? Nick Casey

LEP

Trip to France
List the first and last name of one person that traveled with you? Nick Casey
Which year did you travel? 2015
List two cities you visited Paris, Nice

User Input

Title: Trip to France
Enter the first and last name of one person related to this trip and a hint: Nick Casey, traveled with me
Enter two locations related to this trip and a hint for each: Paris, best art, Nice, wonderful weather

LEP

Trip to France
List the first and last name of one person that traveled with you? Nick Casey
List a location related to "best art" Paris
List a location related to "wonderful weather" Nice

User Studies

- **Performance:**
  - Study strength, recall, reuse
  - Online study, 93 Mturks
  - Asked to create 10 LEPs and 10 passwords and return to authenticate, 3 attempts
- **Friend:**
  - Study if friends can guess LEPs
  - Lab study, 100 pairs of USC students
  - Asked to create 3 LEPs and a friend can guess using personal knowledge, social networks, search engines, 3 attempts

Strength

Measure	LEP Guided	LEP Semi-G	Pass	SQ
Avg. Absolute Strength	161 bit	132 bit	53 bit	< 53bit
Avg. Real Strength (statistical guessing)	99 bit	82 bit	< 53 bit	<< 53bit

LEPs are 29-46 bits stronger than an ideal, randomized, 8-character password

Short-Term Recall

Recall	# of facts	LEP Guided	LEP Semi-G	Pass	SQ
1 week	All-fact	31.6%	45.7%		
	Five-fact	47.7%	45.7%		
	Four-fact	**70%**	**73%**		
	Three-fact	82.1%	89.2%		
	One OP/SQ	-	-	**26%**	**32.1%-83.9%**

LEPs are 2-3 times more memorable than passwords

Long-Term Recall

Recall	# of facts	LEP Guided	LEP Semi-G	Pass	SQ
3-6 mo	All-fact	16.5%	32.3%		
	Five-fact	33.9%	32.3%		
	Four-fact	**53%**	**54%**		
	Three-fact	66.5%	73.6%		
	One OP/SQ	-	-	**9%**	**6.4%-79.2%**

LEPs are 6 times more memorable than passwords

Reuse

Measure	Guided	Semi Guided	OP
Avg. Identical	3.1%	2.7%	5.7%
Avg. Similar	15.4%	4.6%	31.6%

LEPs are reused half as often as passwords

Friend Guessing

Guess	Guided	Semi-Guided	SQs
All-fact	3.5%	0%	-
Five-fact	3.5%	0%	-
Four-fact	**3.5%**	**0%**	**-**
Three-fact	7%	5.3%	-
Security Question	-	-	**17-25%**

Using Mnemonics to Improve Passphrases

with Simon Woo (USC CS)

Mnemonic Passphrase (MNPass)

- Passphrase: sentence or collection of words
  - Longer than password ➔ more secure
  - Different passphrases hard to recall
  - Grammar/popular phrases lower security
- Mnemonic: first letters of each passphrase word
  - Use at authentication: improve memorability (**hint-mnemonic**)
  - Use at creation: improve strength (**guide-mnemonic**)

MNPass Examples

Your passphrase contains words starting with letters MLAAO

Username:

Passphrase:

hint-mnemonic

Your passphrase must contain words starting with the displayed letters

Username:

Passphrase: A B A L O

guide-mnemonic

Passphrase Models

- **UPass:** all user-chosen words
- **UPassHint:** UPass + hint-mnemonic
- **MNPass(0)**: all user-chosen words using guide-mnemonic + hint+mnemonic
- **MNPass(0)-Long**: MNPass(0) + 2-3 more words
- **MNPass(1)**: MNPass(0) with one system-chosen word
- **SysPass:** all system-chosen words
- **SysPassHint:** SysPass + hint-mnemonic

User Study

- Study strength, recall
- Online study, 393 Mturks, 44-66 per model
- Participants assigned randomly into passphrase model, create one passphrase each 5 word long
- Measure recall at 3 and 7 days after creation

Improve Recall

Model	exact match (%)	
	3 day	7 day
w/o hint		
Upass	52.3	40
SysPass	20.7	12.5
w/ hint		
UPassHint	**71.4**	**69.6**
SysPassHint	**26.8**	**18.9**
MNPass(0)	69.7	66.7
MNPass(1)	69.3	67.7
MNPass(0)-Long	66.7	62.8

Good Strength

- Language model (LM) attacker and convert prob. of passphrases into bit-strength entropy

Model	w/o hint	w hint
UPass/UPassHint	61.9	49.3
MNPass(0)	67.5	44.5
MNPass(1)	75.8	60.2
MNPass(0)-Long	84.6	60.3
SysPass/SysPassHint	84.4	63.5

Low Guessability

- Collected 280,550 famous phrases from web
- Compute ordered overlapped words between famous phrases and passphrases

Model	0	1	2	3+
UPass/UPassHint	0	8.4	**39.5**	**52**
MNPass(0)	0	34.8	**60.6**	**4.5**
MNPass(1)	8	50	**38.7**	**3.2**
MNPass(0)-Long	5.9	17.6	**58.8**	**17.6**
SysPass/SysPassHint	0	100	0	0

Summary

Recall

- Hint-mnemonics improve recall by 30–36% after three days and 51–74% after seven days.
- Hints aid recall of important facts.
- MNPass recall is comparable to UPass recall

Strength

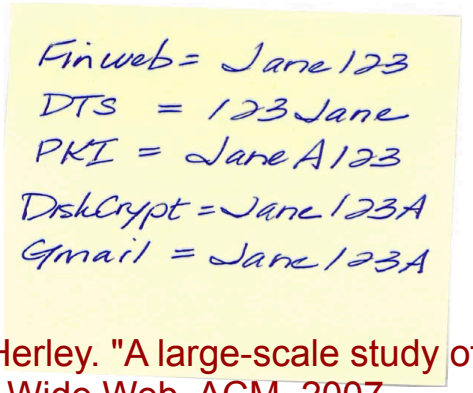
- Mnemonic-guided comparable to system-chosen approach

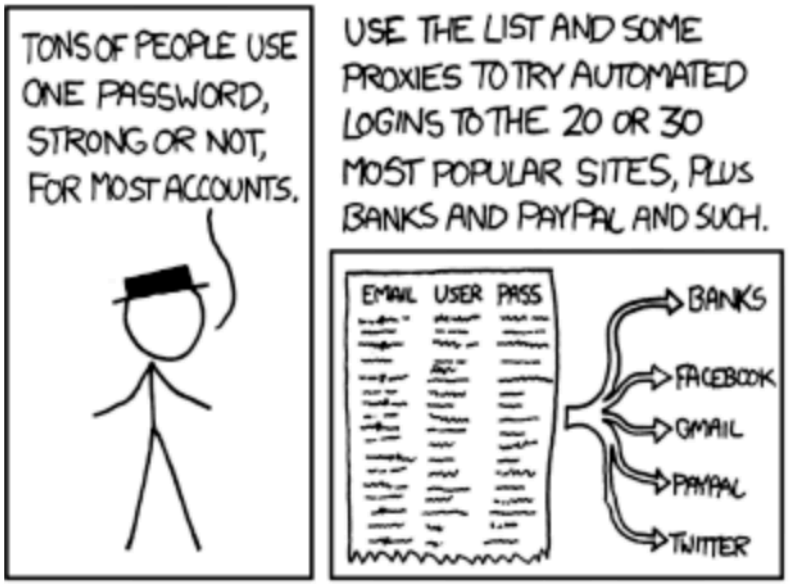
Understanding Password Reuse

with Simon Woo (USC CS), Ameya Hanamsagar (USC CS), Chris Kanich (UIC CS)

Password Reuse

- People remember only 5 or 6 passwords over 30 online accounts[1]
- Cognitive burden (security fatigue) on memorizing multiple passwords
- Many passwords have similar patterns, which can result in password re-use attack





[1] Florencio, Dinei, and Cormac Herley. "A large-scale study of web password habits." Proceedings of the 16th international conference on World Wide Web. ACM, 2007.

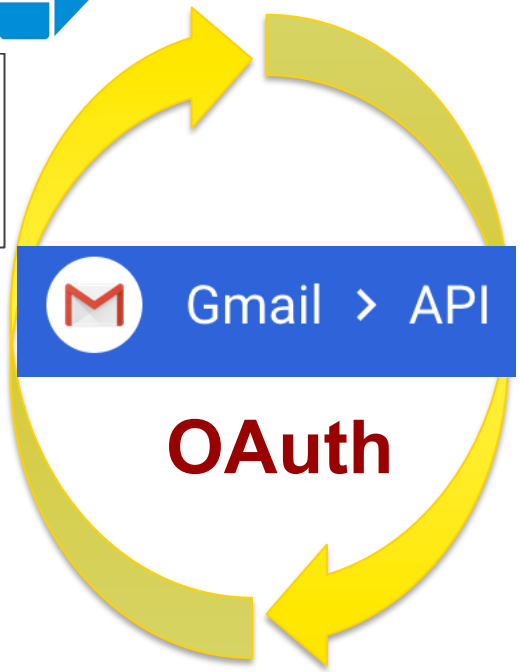
Measure Password Reset Request

CHASE

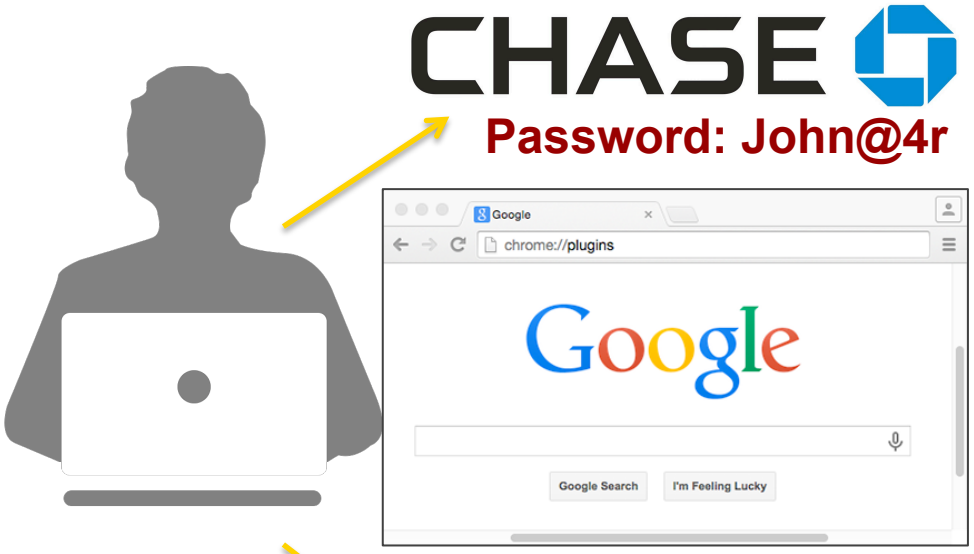
From: chase.com
Message: Pease reset your password

facebook

From: facebook.com
Message: Pease change your password



Detect Similar Passwords



Chrome Extension:
Semantically Transform Passwords

John@4r →Bob#1a
!2jane →?8mary

Preserve user privacy and extract semantics

User Study
(on-going)

- 50 participants
- Let us scan their Gmail account and then attempt to log into 12 sites
- Divide accounts into important (financial/email) and non-important
- Store semantically transformed passwords and ask users about
  - Risk perception
  - Understanding of attacks and reuse

Preliminary Findings

- 83% share passwords between imp/non-imp sites
- Password strength low
  - Users create longer passwords for important sites but they are not stronger
- 90% do not know how automated crackers work
  - Think that they need access to personal information
- Security fatigue leads to reuse – don't care attitude
- Users reveal their important site passwords when failing to log into a non-important site

Conclusion

- Password memorability very important to users
- Users understand security requirements but cannot follow them
- LEPs and mnemonics reasonable solutions to improve memorability and strength of passwords and passphrases
- Need more solutions

Thank You !