An Empirical Study of Mnemonic Sentence-based Password Generation Strategies

Weining Yang, Ninghui Li (Purdue U.) Omar Chowdhury (U. Iowa) Aiping Xiong, Robert W. Proctor (Purdue U.)

Motivation

- Password
 - The most widely used me authentication
 - Easy to understand and u



E	RANK	PASSWORD	CHANGE FROM 2014	
C	1	123456	Unchanged	
	2	password	Unchanged	
u	3	12345678	1 🕅	
	4	qwerty	1 🗷	
	5	12345	2 🖌	
	6	123456789	Unchanged	
	7	football	3 🗖	
	8	1234	1 🖌	
	9	1234567	2 🞵	
	10	baseball	2 🖌	

Motivation

- Need for teaching/training users
 - Creating a difficult-to-guess yet easy-to-remember password is not a skill people naturally possess
 - Hopefully, it is a skill that can be taught

- Research problem
 - What do we teach users? How to teach them?

Need for Password Generation Strategies

Schneier on Security



<u>Blog</u> >

Choosing Secure Passwords

As insecure as passwords generally are, they're not going away anytime soon. Every year you have more and more passwords to deal with, and every year they get easier and easier to break. You need a strategy.

The best way to explain how to choose a good password is to explain how they're broken. The general attack model is what's known as an offline password-guessing attack. In this scenario, the

Advice From Schneier's Essay

Pretty much anything that can be remembered can be cracked.

There's still one scheme that works. Back in 2008, I described the "Schneier scheme":

So if you want your password to be hard to guess, you should choose something that this process will miss. My advice is to take a sentence and turn it into a password. Something like "This little piggy went to market" might become "tlpWENT2m". That nine-character password won't be in anyone's dictionary. Of course, don't use this one, because I've written about it. Choose your own sentence -- something personal.

Here are some examples:

- WIw7,mstmsritt... = When I was seven, my sister threw my stuffed rabbit in the toilet.
- Wow...doestcst = Wow, does that couch smell terrible.

What Do We Know about the Mnemonic Sentence Strategy?

- Studied by Yan et al. in 2000:
 - "Please create a simple sentence of 8 words and choose letters from the words to make up a password. You should put some letters in upper case to make the password harder to guess; and at least one number and/or special character should be inserted as well."
 - An example of such a composition might be using the phrase is "It's 12 noon I am hungry" to create the password "I's12&Iah" which is hard for anyone else to guess but easy for you to remember. By all means use a foreign language if you know one"

How to Assess the Strength of a Strategy?

- Collect passwords created under a strategy from a human subject study
- Apply state-of-art password cracking algorithms to the set and see how many are cracked.
- Adopted in previous works:
 - Yan et al. [2000,2004]; Kuo et al. [2006]; Vu & Proctor [2007]

Problem with Attack-Based Assessment

- Current attack methods are adapted to current password distribution
- Cannot assess the strength of password strategies against attacks targeting it
- Attacks against mnemonic sentence
 - Dictionary attack with passwords created using the strategy
 - Create a dictionary of sentences, and then generate passwords from sentences

How Should We Evaluate a Strategy?

- Each strategy induces a probability distribution over passwords; we should evaluate this distribution.
- If 10,000 users following the strategy chooses (mostly) different password, then good
- If 10,000 users following the strategy result in 100 choose one password, 60 choose another, 45 chose another, etc, then bad

$$\beta$$
-guess-rate (λ_{β})

- Total probability of the most common β passwords $\sum_{i=1}^{\beta} p_D(w_i)$
- Measures the expected success rate for an attacker limited to β guesses per account
- We use $\beta = 1$ and $\beta = 10$

$$\tilde{\lambda}_1 = rac{\operatorname{top}(\mathsf{S})}{|S|}$$
 $\tilde{\lambda}_{10} = rac{\operatorname{top}_{10}(\mathsf{S})}{|S|}$

J. Bonneau, "The science of guessing: analyzing an anonymized corpus of 70 million passwords," in Proceedings of IEEE Symposium on Security and Privacy. IEEE, 2012, pp. 538–552.

Let Us Start Evaluating Such Strategies.

- Use Amazon Mechanical Turk (MTurk)
- Recruit some number (~800) of participants
- Each participant was asked to generate a password using the strategy
 - First type the sentence chosen
 - Then enter password twice

The Mnemonic Strategy We First Assessed

- We use the following instruction, taken from Kuo et al. 2006.
 - 1. Think of a memorable sentence or phrase containing at least seven or eight words. For example, "Four score and seven years ago our fathers brought forth on this continent".
 - Select a letter, number, or a special character to represent each word. A common method is to use the first letter of every word. For example: four ->4, score ->s, and ->&. Combine them into a password: 4s&7yaofb4otc.

How Does the Mnemonic-Sentence Strategy Measure Up?

- Out of 864 participants, 22 chose the same sentence
 - "To be or not to be, that is the question?"
 - 7 chose "2bon2btit?" and 6 chose "2bon2btitq"
- The second most commonly chosen sentence is chosen 9 times
 - "The quick brown fox jumped over the lazy dog"
- Using our metrics, no more secure than Rockyou dataset
- How to avoid this?

Popular Sentences in MneGenEx

Rank	Sentences	Passwords	Frequency
		2bon2btit? (7); 2bon2btitq (6);	
1	to be or not to be, that is the	tbontbtitq (1); 2Bon2Btit? (1);	2.55%
	question (22)	2B0n2bt1tq (1); 2bontbtitq (1);	2.5570
		2brn2btstq (1); 2brn2btit? (1)	
	the quick brown fox jumped over the lazy	tqbfjotld (2); Tqbfjotld (2);	
2		t@bfj0tld (1); tqb4j0tld (1);	1.04%
		TQ35j#TLd (1); tqbfjfld (1);	1.04%
	dog (9)	Tq8fj0tld (1)	
2	one small step for man, one	1ssfm1glfm (3); 1ss4m1gl4m (1);	0.600
3	giant leap for mankind (6)	1\$\$4m1gl4m (1); ossfmoglfm (1)	0.69%

The First Mnemonic Strategy We Assessed (MneGenEx).

- We use the following instruction, taken from Kuo et al. 2006.
 - 1. Think of a memorable sentence or phrase containing at least seven or eight words. For example, "Four score and seven years ago our fathers brought forth on this continent".
 - Select a letter, number, or a special character to represent each word. A common method is to use the first letter of every word. For example: four ->4, score ->s, and ->&. Combine them into a password: 4s&7yaofb4otc.

The Solution: MnePerEx Description

- Think of a memorable sentence or phrase that is meaningful to you, and other people are unlikely to use. The sentence or phrase should contain at least eight words. For example, "I went to London four and a half years ago".
- Select a letter, number, or a special character to represent each word. A common method is to use the first letter of every word. For example: went ⇒ w, four ⇒ 4, and ⇒ &. Combine them into a password: iwtl4&ahya.

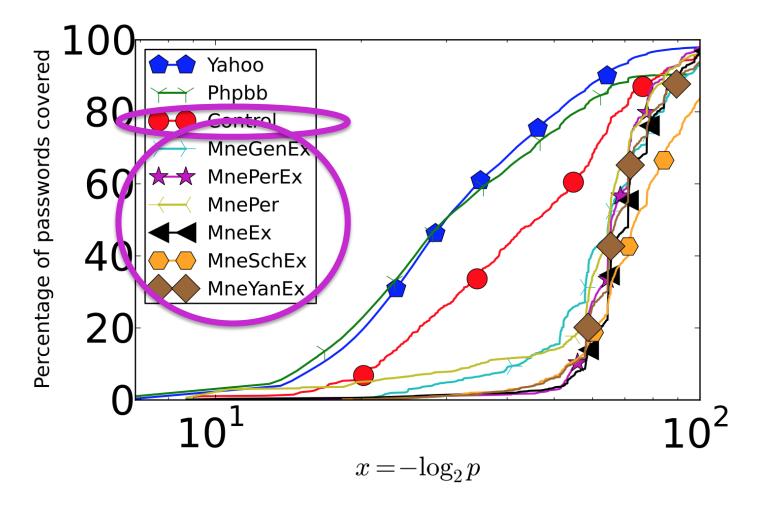
Study Design: Security

- 6 variants of mnemonic strategies and 1 control group
- MneGenEx: With Gettysburg address ex
- MnePerEx:
- MneSchEx:
- MneYanEx:
- MnePer:
- MneEx:

Personalized with examples

- Schneier's instructions
- Instructions used in Yan et al.
 - Personalized, no examples
 - No emphasis on personalization, lots of personalized examples

Password strength measured by Probability Threshold Graph



Collision Evaluation of Mnemonic Strategies

	Count	$ ilde{\lambda}_1$ (top)			$ ilde{\lambda}_{10}$ (top ₁₀)		
Strategy		Sentence	Password		Contonoo	Password	
			Case	Case	Sentence	Case	Case
			Insensitive	Sensitive		Insensitive	Sensitive
MneGenEx	864	2.5%(22)	0.9%(8)	0.8%(7)	7.8%(68)	5.3%(46)	4.1%(36)
MnePerEx	777	0.1%(1)	0.1%(1)	0.1%(1)	1.3%(10)	1.3%(10)	1.3%(10)
MnePer	745	0.7%(5)	2.3%(17)	2.3%(17)	2.8%(21)	5.8%(43)	5.6%(42)
MneEx	868	0.7%(6)	0.2%(2)	0.2%(2)	2.2%(19)	1.7%(15)	1.3%(11)
MneSchEx	753	0.4%(3)	0.5%(4)	0.3%(2)	2.8%(21)	1.7%(13)	1.5%(11)
MneYanEx	799	0.3%(2)	0.3%(2)	0.3%(2)	1.6%(13)	1.5%(12)	1.4%(11)
Control	678	N/A	1.2%(8)	0.9%(6)	N/A	3.4%(23)	2.9%(20)

Evaluation on MnePerEx

	Strategy	Count	$ ilde{\lambda}_1$ (top)			$ ilde{\lambda}_{10}$ (top_10)		
			nt Sentence	Password		Contonoo	Password	
				Case	Case	Sentence	Case	Case
				Insensitive	Sensitive		Insensitive	Sensitive
	MneGenEx	864	2.5%(22)	0.9%(8)	0.8%(7)	7.8%(68)	5.3%(46)	4.1%(36)
	MnePerEx	777	0.1%(1)	0.1%(1)	0.1%(1)	1.3%(10)	1.3%(10)	1.3%(10)
	MnePer	745	0.7%(5)	2.3%(17)	2.3%(17)	2.8%(21)	5.8%(43)	5.6%(42)
	MneEx	868	0.7%(6)	0.2%(2)	0.2%(2)	2.2%(19)	1.7%(15)	1.3%(11)
	MneSchEx	753	0.4%(3)	0.5%(4)	0.3%(2)	2.8%(21)	1.7%(13)	1.5%(11)
	MneYanEx	799	0.3%(2)	0.3%(2)	0.3%(2)	1.6%(13)	1.5%(12)	1.4%(11)
	Control	678	N/A	1.2%(8)	0.9%(6)	N/A	3.4%(23)	2.9%(20)

Which Matters: Personalized Examples or Instructions?

- MnePer: asks for personalized choice of sentences in instructions, but gives no example
 - Think of a memorable sentence or phrase that is meaningful to you, and other people are unlikely to use. The sentence or phrase should contain at least eight words.
 - 2. Select a letter, number, or a special character to represent each word, and combine them to create the password.

MneEx: provide several personalized sentences as examples.

- "In June 2013, my wife and I visited Tokyo, Kyoto, and Sapporo" might become "i63mw&ivTk&\$".
- *"Run 5 miles per week for my first half marathon"* might become *"r5mpw4mfhm"*.
- "My high school classmates had a reunion in July 2014" might become "Mhscharij2".
- "I sold my gold Toyota corolla when it had close to 120000 miles" might become "i\$mgtcwlhc21m".
- "Danny bought the book The Razor's Edge from me for five dollars" might become "Dbtbtrefm45d".
- "Save money for traveling with my parents to Germany" might become "S\$4twmp2G".

MnePer, MneEx

	Count	$ ilde{\lambda}_1$ (top)			$ ilde{\lambda}_{10}$ (top ₁₀)		
Strategy		Sentence	Password		Contonos	Password	
			Case	Case	Sentence	Case	Case
			Insensitive	Sensitive		Insensitive	Sensitive
MneGenEx	864	2.5%(22)	0.9%(8)	0.8%(7)	7.8%(68)	5.3%(46)	4.1%(36)
MnePerEx	777	0.1%(1)	0.1%(1)	0.1%(1)	1.3%(10)	1.3%(10)	1.3%(10)
MnePer	745	0.7%(5)	2.3%(17)	2.3%(17)	2.8%(21)	5.8%(43)	5.6%(42)
MneEx	868	0.7%(6)	0.2%(2)	0.2%(2)	2.2%(19)	1.7%(15)	1.3%(11)
MneSchEx	753	0.4%(3)	0.5%(4)	0.3%(2)	2.8%(21)	1.7%(13)	1.5%(11)
MneYanEx	799	0.3%(2)	0.3%(2)	0.3%(2)	1.6%(13)	1.5%(12)	1.4%(11)
Control	678	N/A	1.2%(8)	0.9%(6)	N/A	3.4%(23)	2.9%(20)

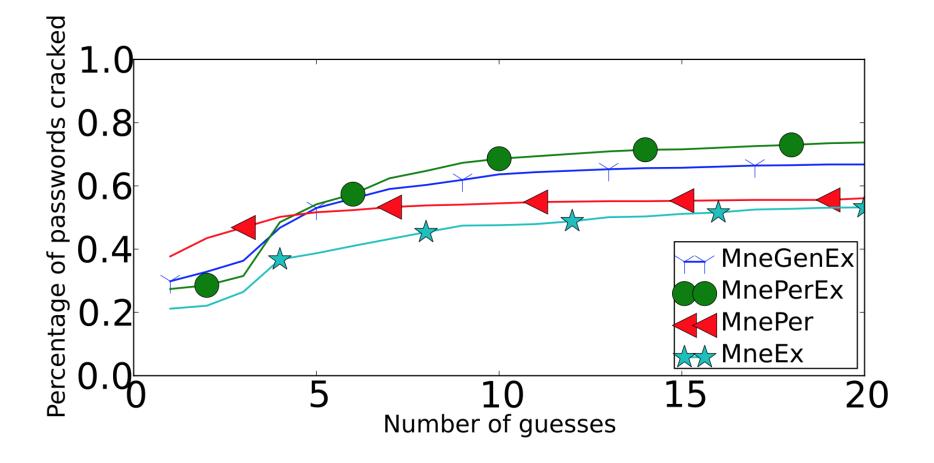
Evaluation on MneSchEx, MneYanEx

	Count	$ ilde{\lambda}_1$ (top)			$ ilde{\lambda}_{10}$ (top ₁₀)		
Strategy		Sentence	Password		Contorro	Password	
			Case	Case	Sentence	Case	Case
			Insensitive	Sensitive		Insensitive	Sensitive
MneGenEx	864	2.5%(22)	0.9%(8)	0.8%(7)	7.8%(68)	5.3%(46)	4.1%(36)
MnePerEx	777	0.1%(1)	0.1%(1)	0.1%(1)	1.3%(10)	1.3%(10)	1.3%(10)
MnePer	745	0.7%(5)	2.3%(17)	2.3%(17)	2.8%(21)	5.8%(43)	5.6%(42)
MneEx	868	0.7%(6)	0.2%(2)	0.2%(2)	2.2%(19)	1.7%(15)	1.3%(11)
MneSchEx	753	0.4%(3)	0.5%(4)	0.3%(2)	2.8%(21)	1.7%(13)	1.5%(11)
MneYanEx	799	0.3%(2)	0.3%(2)	0.3%(2)	1.6%(13)	1.5%(12)	1.4%(11)
Control	678	N/A	1.2%(8)	0.9%(6)	N/A	3.4%(23)	2.9%(20)

Cracking passwords from mnemonic strategies

- Guess passwords from sentences
 - Learn word->character conversion from training dataset.
 - Normal words: use the first character of the word (and with LEET conversion).
 - Special words: based on pronunciation or meaning. For example: too->2, first->1, question->?, and->&

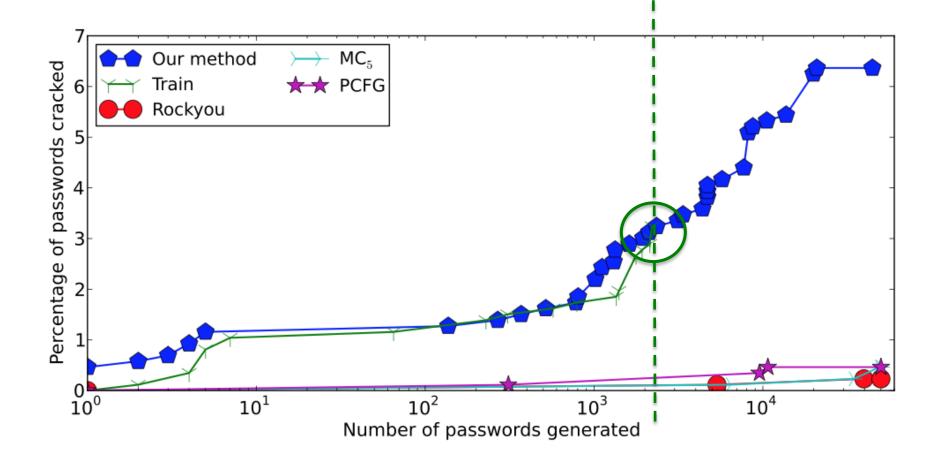
Cracking passwords when knowing sentences



Cracking passwords from mnemonic strategies

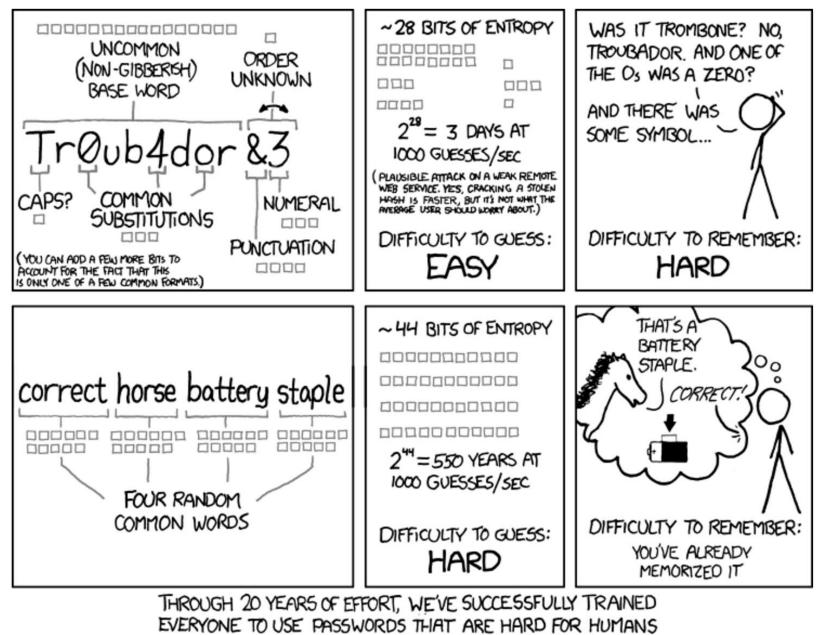
- Cracking from scratch
 - Guess sentences based on dictionary attack using sentences chosen in the training set as dictionary
 - Guess passwords from sentences.

Cracking passwords from mnemonic strategies



Findings

- The exact instructions describing the strategy and the examples matter very much.
- Using generic instructions and examples results in weak passwords.
- Instructions specifically requesting personalized sentences and containing appropriate examples lead to strong passwords.
- Both personalized instructions and examples are needed.



TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

THANK YOU

Datasets on mnemonic strategies available for sharing. Email me (ninghui@purdue.edu).

Questions?