DESIGNING AND CRACKING ASSOCIATIVE PASSWORDS

KIRSI HELKALA
ASSOCIATE PROFESSOR
GJØVIK UNIVERSITY COLLEGE

Kirsi Helkala and Nils Kalstad Svendsen.
The Security and Memorability of Passwords Generated by Using an Association Element and a Personal Factor.
In proceedings of NordSec 2011 and
LNCS 7161, pp.114-130. Springer, Heidelberg, 2012.

Kirsi Helkala, Nils Kalstad Svendsen, Per Thorsheim and Anders Wiehe.
Cracking Associative Passwords.
In LNCS, vol.7617, Secure IT Systems:
17th Nordic Conference, NordSec 2012.
Proceedings: Springer, p. 153-168.

Content

- Motivation
- Experiment 2011
- Guidelines for Associative Passwords
- Description of the Collected Data
- Cracking Experiment 2012
- Conclusion

Motivation

- At NordSec 2011, we reported an experiment where association was successfully used in creation of memorable and strong passwords
- *The fact that these passwords might contain information that can be derived from the login sites or have a repeated structure has been a source of criticism of the security of associative passwords*
- We addressed these possible drawbacks by challenging the passwords as *MD5crypt representatives* with the open source password-cracking tool, *John the Ripper*
- MD5 representatives were used in a public challenge to the password-cracking community

EXPERIMENT 2011

- Engineering B.Sc. Students
  - Age 19-25
  - All except one Norwegian
- Three phases
  - Phase 1: Education
  - Phase 2: Password design
  - Phase 3: Recall

- Collected 508 associative passwords, further used in Cracking Experiment 2012

Design Guidelines For Associative Passwords

1. Identify element associated to the service
2. Identify Personal Factor
3. Create password in one of the listed categories:

Word password:

- Minimum 13 characters
- Use many short and modified words
- Remember special characters when modifying
- The longer the password, the less modification is needed

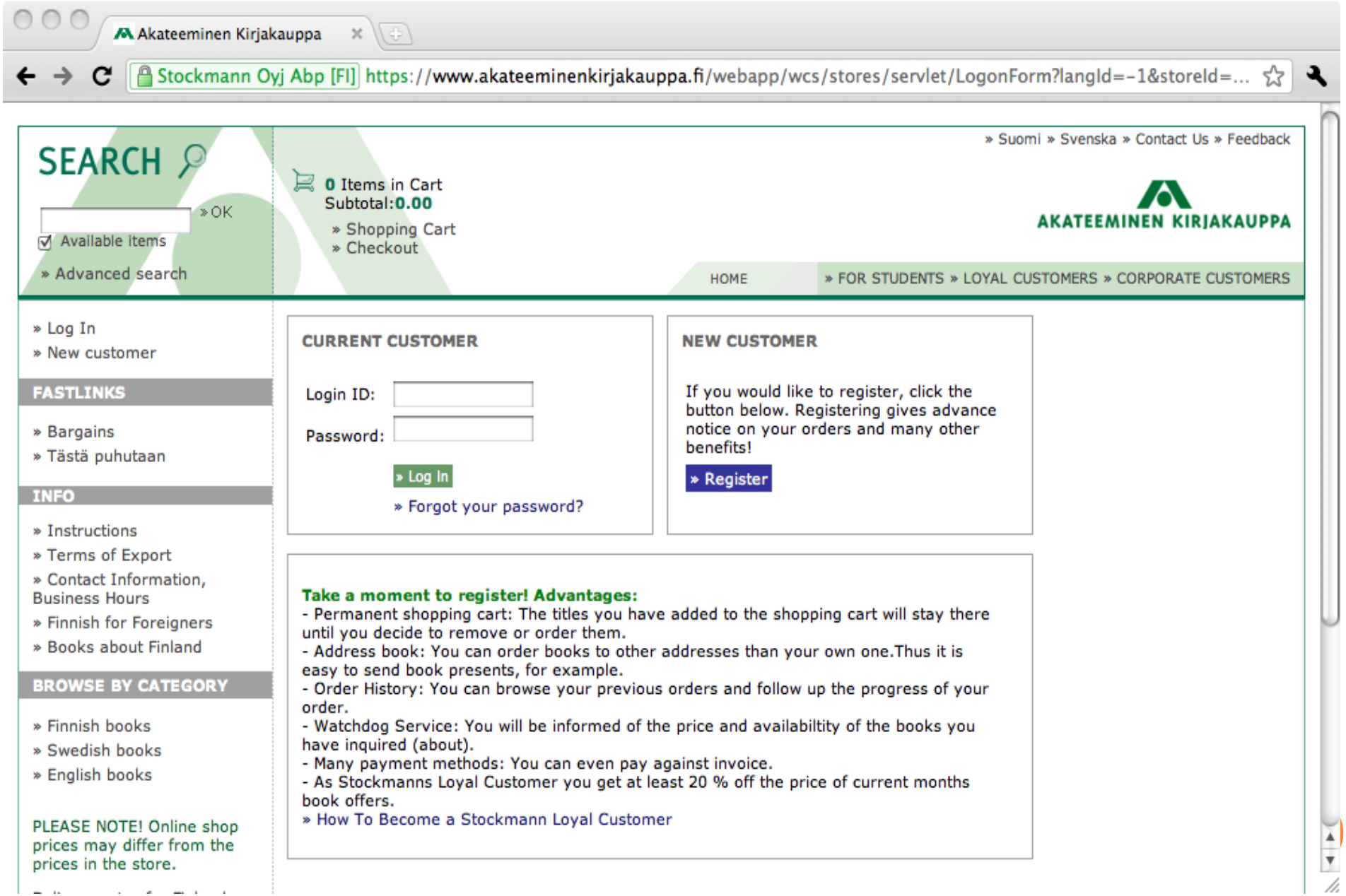
Design Guidelines

Mixture password:

- Minimum 11 characters
- Use several short (not the same length), modified words together with extra characters from large character set
- Remember special characters when modifying

Non-word password:

- Minimum 9 characters
- Use characters from all character sets but in such way that there are many special characters


Akateeminen Kirjakauppa
Stockmann Oyj Abp [FI] https://www.akateeminenkirjakauppa.fi/webapp/wcs/stores/servlet/LogonForm?langId=-1&storeId=...
SEARCH
» OK
Available items
» Advanced search
0 Items in Cart
Subtotal:0.00
» Shopping Cart
» Checkout
» Suomi » Svenska » Contact Us » Feedback
AKATEEMINEN KIRJAKAUPPA
HOME
» FOR STUDENTS » LOYAL CUSTOMERS » CORPORATE CUSTOMERS
» Log In
» New customer
FASTLINKS
» Bargains
» Tästä puhutaan
INFO
» Instructions
» Terms of Export
» Contact Information, Business Hours
» Finnish for Foreigners
» Books about Finland
BROWSE BY CATEGORY
» Finnish books
» Swedish books
» English books
PLEASE NOTE! Online shop prices may differ from the prices in the store.
CURRENT CUSTOMER
Login ID:
Password:
» Log In
» Forgot your password?
NEW CUSTOMER
If you would like to register, click the button below. Registering gives advance notice on your orders and many other benefits!
» Register
Take a moment to register! Advantages:
- Permanent shopping cart: The titles you have added to the shopping cart will stay there until you decide to remove or order them.
- Address book: You can order books to other addresses than your own one.Thus it is easy to send book presents, for example.
- Order History: You can browse your previous orders and follow up the progress of your order.
- Watchdog Service: You will be informed of the price and availabiltity of the books you have inquired (about).
- Many payment methods: You can even pay against invoice.
- As Stockmanns Loyal Customer you get at least 20 % off the price of current months book offers.
» How To Become a Stockmann Loyal Customer

Some Associative Passwords

- Associated: Triangle and circle in a logo
  - Triangle=V and circle=O
- Personal factor
  - Princess with a golden ball, 1984
- Word:

  Tri@ngleCirclePricessWith@GoldenB@ll
- Mixture:

  V&O/Princess_With_a_Golden_Ball84
- Non-word:

  V&O/Pwagb_84

  VP&rOi8n4cess

Description of the Collected Data that might have Effect on Successful Cracking

LANGUAGE

- 60.0% of the passwords were generated using only Norwegian
- 19.9% were based on English
- 9.3% were based on Finnish words
- 8.9% were bilingual passwords being mostly Norwegian-English

- *This indicates that users' first option for the language is their mother tongue.*

MODIFICATION

- 90-91% of Word and Mixture passwords were modified
- Most common modification (60%) was capitalization
- The modifications were very similar to Leet-alphabets

Original	**a**	**d**	**e**	**g**	**h**	**i, l**	**o**	**s**	**t**	**u**	**å**	**ø**
Replaced with	4, @	L	3, €	6	|-|	1	0, ø	5, z, $	7	|_|	@, aa, \a	O e, o, @, \o
Original	1	3	&	to	se	eight	og					
Replaced with	i	e	3	2	z	8	&					

ASSOCIATION ELEMENTS

- Primary: 57%, Secondary: 26%, Tertiary: 17%

- About password
  - ➔85.8% began with a letter
  - ➔17% began with the same letter as the site
  - ➔84.1% of starting letters were upper case letters
  - ➔31.3% of all of the passwords contained the name of the site in one form or another

  - ➔10.8% of passwords in our dataset included a colour word and 65.5% of these passwords were associated with sites that used strong colour(s)

PERSONAL FACTORS

- No factor: 15%
- Service related: 14%
- Site related: 5%
- Not related: 66%

- No same factors among participants

- Personal factors varied considerably and most of them were information that is rather difficult to find

PASSWORD SEMANTICS

- Word: $Word_1 Word_2 \ldots Word_n$
  - Words are pure or modified
  - MyOwnStrongPassword
- Mixture: $Nw_0 Word_1 Nw_1 Word_2 Nw_2 \ldots Nw_{n-1} Word_n Nw_n$
  - Words are pure or modified
  - Nw:s are meaningless char strings with variable lengths
  - !My#Own#Strong#Password!
- Non-word: $C_1 C_2 \ldots C_n$
  - C:s are characters from all character sets
  - !M#0#S# P!

Wondering about Memorability?

Effect of the Association Element on Memorability

- Group 1 (study 2008-2009):
  - one password without association
  - a recall percentage of 31%
- Group 2:
  - ten passwords with association
  - a recall percentage of 49%

- Analysis shows that the data provides sufficient evidence to conclude that *use of an Association Element has positive effect on the memorability of the password.*

Memorability vs. Strength - 1

Category	Fully Remembered	1-2 errors	Not Remembered
Good ones	61.7%	14.9%	23.4%
Weak ones	47.5%	15.7%	36.8%

	1. Recall Session		2. Recall Session	
Category	Fully Remembered	1-2 errors	Primary	Secondary
Word	38.8%	13.6%	42.5%	44.0%
Mixture	48.6%	16.8%	40.5%	48.0%
Non-word	64.5%	14.8%	66.4%	50.0%

CRACKING EXPERIMENT

JOHN THE RIPPER, PART I

- In the first three approaches, *MD5crypt with salt* was used to hash the passwords
- The *same salt* was used for all the passwords

- The machine used was Intel(R) Core(TM) i7-2760QM CPU @ 2.40GHz with CentOS operating system
- The computer had alternative tasks to handle during the experiment, which reduced the cracking speed

CRACKING 1

- We combined *English and Norwegian wordlists* from Aspell in the newest version of Fedora
- The wordlists were used to run John the Ripper in *wordlist mode* adapted with MD5 hash rules
- With this mode, we were immediately *able to crack 3 out of 508 passwords; all very weak*
  - First one was 8 character long password, which only contained digits
  - Second one was a name of an English town with first letter capitalized
  - Third password was a name of a Norwegian community with first letter capitalized

CRACKING 2

- Used John the Ripper in *incremental mode*
- Let it run for a week at approximately 40M c/s
- Were able to crack *eleven of the remaining 505 passwords; all very weak*
  - All of the identified passwords were shorter than eight characters

- There were several other passwords with less than eight characters, but they were not found within the time frame and had the following properties:

CRACKING 2 CONTINUES

- 5 chars:
  - Two mixture pwds, both having word part with first letter capitalized and non-word part in the end including a special char
  - One was totally capitalized non-word password
- 6 chars:
  - Three totally capitalized non-word pwds
  - One was a word pwd containing two words with capitalization and not so common modification (! @)
- 7 chars:
  - Four non-word pwds containing uc's, lc's and digits
  - One mixture pwd containing not so common modification and ending to non-word part with two digits

CRACKING 3

- Used reduced wordlist
  - The participants had registered their associations, and we used this information to generate a new wordlist
  - This list contained 247 elements, mostly words, but also digits, symbols and Internet addresses
- NOTE: the list contained *all three types of association elements*
  - If an adversary makes such a list, we can assume that he is able to include the primary associations easily
  - However, including the secondary and tertiary associations would need a great deal of guessing
- *This implies that a potential attacker would have a larger wordlist than the one we used as input*

CRACKING 3 CONTINUES

- Used modifications shown earlier were user as rules for John the Ripper (excluded: eight ➔ 8 and og ➔ & etc.)
- Used "between characters" collected from the data between words in Mixture passwords (shown below)
- Limited to passwords containing one, two or three words, separated with a between character
- Final wordlist (yet to be mod.) contained 3 391 490 557 raw combinations
- In our dataset 107 (21%) passwords full filled this requirement (five of these had been found earlier and were excluded from the search list)

<no char>	<space>	,	.	-	_	+	/	\	?	!	#	@	<	>

CRACKING 3 CONTINUES

- The run took six days, four hours and twenty-six minutes
- The speed at the end was twenty-five million trials per second: at least $13*10^{12}$ trials
- *Were able to crack only one additional password*
  - a three-letter word with first letter capitalized
- Reasons for not finding more:
  - ➔Grammatical errors, lacking grammatical alternatives
  - ➔Used personal factors were not site related
  - ➔Full sentences, more words missing from the list
  - ➔Same characters modified differently
  - ➔Strange capitalization

CRACKING CHALLENGE

- We challenged the password-cracking community by publishing nine examples of the password MD5 hash without salt on the Security Nirvana blog site
- From each category: *Word, Mixture and Non-word*, we included *one weak, one good and one strong password*
- All passwords *were also recalled* by the users in the previous study 2011
- Examples of each category were given on the introduction part of the blog post
- *None of them has been revealed yet*

JOHN THE RIPPER, PART II

- A targeted attack against *three Word- passwords* which also were part of the open challenge
- Created a new list containing 156 word containing word association, common verbs, nouns prepositions so that meaningful sentences could be created
- *Also personal factors were included* this time
- NOTE: this was possible only for us knowing the data
- *Able to crack one out of three*
- Two were left unfound due to simultaneously modifications of different characters, something that the cracking mode was not able to handle

EXAMPLES OF PWD STRUCTURES IN THE CHALLENGE

IWishAcademicSuccess (Cracked by us)

HvitH0ur3L4si (white hour eglass)

Th3M1dd3l4ld3r3nS3tt3rs (the middel alderen setters)

COLLEGEF546

j36#5k@1#p\a#F3R1 (jeg skal på ferie)

S@l?In@2012TtI? (salaatti, Ina, 2012)

RV5BC6T379

HhpaMkhkh77 (Heppa huokaili peiton alla Mielellä kovin haikealla kh77)

Ssomoymkik7e7# (Suomi 77, smykke #)

CONCLUSIONS

- Passwords based on primary associations were assumed to be easiest to crack, since, in theory, one can generate a list containing "all" associations of a service site
- However, it is not enough to have a list of "all" associations
- *Passwords become memorable when the associated words are linked to each other logically, meaning that sentences are used*
- *As a consequence, other words, such as verbs and pronouns have to be added to the dictionary leading to a larger set of words and increased complexity*

CONCLUSIONS

- We recommend the use of *associative passwords with secondary and tertiary associations combined with guidelines for categorized passwords* for creating memorable and strong passwords
- Furthermore, users should always be encouraged to *use both a personal factor and an association element*
- By doing so, adversaries are forced to use a large word set, which makes the cracking task more difficult