Random Password Generators

Michael Leonhard uic@tamale.net
V.N. Venkatakrishnan venkat@cs.uic.edu

Department of Computer Science
University of Illinois at Chicago

IEEE Electro/Information Technology Conference
2007

Everyday Random Passwords

Random Password: a password created for you by a machine

- Bank card PIN
- Online banking assigned login ID
- Forgot your password? Get a new (random) one by email.

Outline

Passwords Are Important

- Password authenticates user to application.
- Break-ins harm two parties:
  - User (SSN, Name, Address, Reputation)
  - Application (Site Content, Trade Secrets, Liability)
- Applications have a big stake in password security.
- Yet, users choose their passwords.

User Motivation

Example: www.NewYorkTimes.com

Password is a nuisance to user. User not motivated to use a good password.

Example: www.MidAmericaBank.com

Password protects user's money.

Attacking Passwords

- Guess
- Intercept at User's computer
- Intercept on Network
- Crack application, recover Password Hashes "Chicago08": 0x26ba841da2ec8b6118ab63f1ea281d...61f6
- Attack another application, recover reused password

Reusing Passwords

Using one password for multiple applications.

- Attacker cracks easy target (myspace.com), learns passwords of hard target (bank.com)
- Application can stop reuse by assigning a password
- Limitation: person can reuse on future accounts

Password Entropy

How to measure the randomness of a password?

- Generator chooses password p from S, set of all potential passwords
- $|S|$ is the number of possible passwords
- $log_2|S|$ is the bits of entropy in p

Example

Choose p from the set $S = \{a, b, c, d, e, f, g, h\}$.
$|S| = 8$ so p has 3 bits of entropy.
Each element must have the same chance of being chosen.

Thought-Up Passwords

Think up a password with mixed-case letters and numbers. It probably has:

- Words
- Capital letters starting words
- Numbers at end

Paris98	GummyBear55	GoSox2007

Problem: these are in cracking dictionaries
$\Rightarrow$ Offline Attack is Easy

Think-Up Phrase-based Passwords

"O Romeo, Romeo! wherefore art thou Romeo?" $\Rightarrow$ "ORRwatR?"

"1. A robot may not injure a human being . . ." $\Rightarrow$ "1Armniahb"

- Problem: same weakness as regular thought-up passwords
- The Attack: Harvest phrases from the Web, make a cracking dictionary
- See paper by Kuo, Romanosky, and Cranor in SOUPS'06

Our Objectives

We want to study three random password generation schemes.

while paying attention to:

- *Security*.
- *Memorability*.
- *User Affinity*.

Security studied through entropy analysis of the schemes.

Memorability and affinity through actual usability study we conducted.

Scheme 1: Random Characters (AlphaNum)

Use software to choose letters and numbers.

dVysgZ	a1LCLQ	EDaL8p

- Every password is equally probable
  $\Rightarrow$ GOOD SECURITY (35.7 bits of entropy)
- Good: very short
- Bad: hard to memorize

Sch.2: Random Words (Diceware)

Word List

. . .
16666 clerk
21111 cliche
21112 click
21113 cliff ←
21114 climb

plaid hey benz fog bribe briny doe slim dodo

- Every sequence of words is equally probable
  $\Rightarrow$ GOOD SECURITY (38.8 bits of entropy)
- Good: easy to remember
- Bad: long (for typing)

3: Random Syllables (Pronounce3)

Templates

$\alpha\beta\beta\alpha\beta\alpha\beta\alpha$,
$\alpha\beta\beta\alpha\alpha\beta\beta\alpha$,
$\beta\alpha\alpha\beta\alpha\beta\beta\alpha$,
$\beta\alpha\alpha\beta\beta\alpha\beta\alpha$,
$\beta\alpha\beta\alpha\alpha\beta\beta\alpha$,
$\beta\alpha\beta\alpha\beta\alpha\beta\alpha$,
$\beta\alpha\beta\alpha\beta\beta\alpha\alpha$

Vowels

a, e, i, o, u

$\Rightarrow \quad \alpha\beta\beta\alpha\alpha\beta\beta\alpha \quad \Rightarrow$ adpoaska

Consonants

b, c, ch, d, f, g, h, j, k, l, m,
n, p, ph, r, s, st, v, w, x, y, z

- Every word has equal chance
  $\Rightarrow$ GOOD SECURITY (30.8 bits of entropy)
- Good: easy to remember

Which Generator is Best?

Metrics:

- Security: Amount of entropy in each password
- Memorability: Can you remember the password?
- Affinity: Do you like the password?

The Experiment

Subjects: students in a class on computer security

Questionnaire 1:

- Your assigned password is: adpoaska
- Write it, solve these puzzles, write it again

Password Memorability Study Questionnaire #1
October 16, 2006
Michael Leonhard

Thank you for participating in this study of password generators. This study compares the quality of passwords generated by various algorithms. You will act as a user of a website. The website generates a random password for you. You will memorize this password by writing it several times. After two weeks, on October 30, you will need to remember the password and log into the website. Please treat this password as you would any normal password of yours. Your participation is greatly appreciated.

Please write your name: _____

Please pretend that you have registered on a website called Joe Maxwell Internet Auctions.

Joe Maxwell
Internet Auctions

Thank you for registering. Your password is: **a1LCLQ**

To help you memorize your password, please write it in the login box below.

Joe Maxwell

Please take a moment and count from 1 through 42 in your mind. Then login again:

Joe Maxwell Internet Auctions

Login

Password: [ ]

[Login]

Now please solve the following set of equations for y:

$2x = 102 - 2y$
$x = 2y + 42$

Now login again:

Joe Maxwell Internet Auctions

Login

2 weeks pass. . .

Questionnaire 2:

- Remember your assigned password, write it
- Please answer these questions

Password Memorability Study Questionnaire #2
October 30, 2006
Michael Leonhard

Thank you for participating in my study of password generators! Two weeks ago, you received a sheet like this one. Using that sheet, you registered at Joe Maxwell Internet Auctions, received a password, and practiced logging in. This sheet is the second part of the study. If you choose to participate in this part of the study, please try to remember your password and log in again. If you do not wish to participate, please leave the sheet blank. I will keep your names and individual performance secret. I greatly appreciate your participation.

Please write your name: _____

Please pretend that you have returned to Joe Maxwell Internet Auctions website. Try to remember your password and write it in the box below.

Joe Maxwell Internet Auctions

Login

Password: [ ]

[Login]

Please log in again. If you are unsure of your password, please try a different one.

Please log in again. If you are still unsure of your password, please try a different one.

Joe Maxwell Internet Auctions

Login

Password: [ ]

Login

Please circle your answers to the following questions:

Did you remember your password?

yes probably don't know probably not no

Did you write your password on the questionnaires? yes no

Did you write your password somewhere else? yes no

How do you like your password?

hate it don't like it ok like it love it

How did you remember your password?

Results

- 19 Participants completed both questionnaires.

	AlphaNum	Diceware	Pronounce3
Assigned	6	7	6
Recalled (0 errors)	1	2	1
Recalled (1 error)	2	0	1

- Questionnaire 2 yielded much valuable feedback

Related work

Bunnel et al (CS'97) performed a similar study.

- schemes were simpler than ours.

Pwdgen (Security'05), PwdMultiplier (SOUPS'06) - schemes for generation / storage of online passwords.

- Both criticized in usability study by Chiasson et al (Security'06).

U.S. DoD guidelines on password security.

- Our technique for analyzing passwords based on this study.

What We learned

- How to improve the generators to reduce errors
- Usability studies should employ real applications, used regularly
  - We have created a WordPress plugin for using random passwords
- Users accept assigned passwords

Conclusion

Assigned Random Passwords are a valuable tool for increasing application security.

More Information

http://tamale.net/pub/2007/pwdgen/

Thanks To

The students of Network Security, Fall 2006