Reusable Passwords:
It's Time to Retire “Open Sesame”

Bruce K. Marshall, CISSP

bkmarsh@feist.com

www.feist.com/~bkmarsh

Introduction

- Computer security continues to grow in necessity and value to corporations.
- Authentication systems tend to receive less attention than they need
- We are getting closer to a critical point in time where reusable passwords won’t be as effective as our environments demand
- Overview

Identification & Authentication

Identification, the process of announcing who you are, provides very little security value by itself.

“Without authentication, user identification has no credibility.”
- DOD Password Management Guideline

Authentication is the process of obtaining and validating proof of a user’s given identification.

Authentication

Authentication’s place in the security model:

- Authentication should take place before the user is granted any rights or privileges.
- This is typically accomplished by prompting the user for a secret phrase, or password, that only they should know.
- Authentication processes usually constitute one of the first, and most effective, methods of securing a system.
- Hackers don’t even need to know much about your particular OS to try username/password combinations – Hack FAQ

Authentication

The indifference of users is one of the biggest factors hurting the strength and usefulness of authentication systems.

Authentication system components / weaknesses

1. Password input
2. Password transportation
3. Password verification/storage
4. Passwords themselves

However, #1-#3 are of less value if #4 is weak

We’ll focus our attention on #4

Types of authentication

- What you know: knowledge
- What you have: possession
- What you are: self

What you know - Authentication

- Reusable passwords are the most prevalent form of “what you know” authentication.
- The majority of the time, the user is allowed to specify what they want to use as a password.
- On occasion, the user is assigned a machine or admin. generated password.

What you know - Authentication

Benefits

- Cheap: comes built into almost every information system.
- Simple: No real knowledge curve or culture changes required to implement.
- Common: Richest knowledge base on mgmt.
- Secure - to a point: Obviously better than nothing, but we'll go into detail on that.

What you know - Authentication

Disadvantages

- Disclosure: Easy and common for a user to accidentally or purposely divulge their password.
- Guessable: Susceptible to brute-force search attacks.
- Limited Security: The more strength a password has also tends to make it harder to remember (which usually results in the user writing it down somewhere).

What you know - Authentication

Additional Disadvantages

- Technology has become the very tool of hackers. Brute-force speed can easily double within years.
- Relies on the end user to ensure authentication system integrity.
- Limited lifetime means you need to enforce frequent changes - users typically react by writing down passwords or choosing similar ones each time.

Introduction to the Study

Premise:

To provide some hard data and statistics on normal password choices and their inherent weaknesses to the information security community.

Introduction to the Study

Why is this data important?

It provides information that can be used for:

- Internal testing of password security
- Justifying authentication system investments
- Secure system design & implementations guidelines

Introduction to the Study

Study parameters

- 3,163 unique user accounts w/ plaintext passwords
- Users were initially allowed to specify their passwords verbally to a computer help desk. Policy failure
- If the user was knowledgeable enough, they could change their own password later
- Passwords had to be between 3 and 12 characters, this was enforced by the OS. No other restrictions existed.

RP Study - Character Sets

There are essentially 4 character sets that passwords can consist of:

• Numeric	10
• Alphabetic	26
• Case-sensitive Alphabetic	52
• Extended (w/ [space])	33
Maximum possible	<u>95</u>

RP Study - Character Sets

You can find the total number of potential character combinations in a fixed length password by taking the number of available characters (X) to the power of the number of fields (Y).

Thus if you have a 6 character password consisting of all lowercase alphabet letters:

X^Y is $26^6 = 308{,}915{,}776$ possibilities

RP Study - Character Sets

The total number of potential character combinations in a variable length password if found by taking the number of available characters (X) to the power of the lowest number of fields (Y) added incrementally to the power of the highest number of fields (Z)

If you have a 1-6 character password consisting of all lowercase alphabet letters:

$X^Y + \ldots + X^Z$ is $26^1 + \ldots + 26^6 = 321{,}272{,}406$

RP Study - Character Sets

1-6 length passwords yield these possibilities:

- **Alpha (26^6): 321,272,406**
- **Upper/lowercase alpha (52^6): 20,158,268,676**
- **Numeric (10^6): 1,111,110**
- **Upper/lower case alpha + numeric (62^6): 57,731,386,986**
- **Extended (32^6): 1,108,378,656**
- **Upper/lower case alpha + numeric + extended (95^6): 742,912,017,120**

RP Study - Character Sets

1-8 length passwords yield these possibilities:

- **Alpha (26^8): 217,180,147,158**
- **Upper/lowercase alpha (52^8): 54,507,958,502,660**
- **Numeric (10^8): 111,111,110**
- **Upper/lowercase alpha + numeric (62^8): 221,919,451,578,090**
- **Extended (32^8): 1,134,979,744,800**
- **Upper/lowercase alpha + numeric + extended (95^8): 6,704,780,954,517,120**

RP Study - Character Sets

Number & percentage of passwords with:

• Lowercase	2,745	86.8%
• Uppercase	1,737	54.9%
• Numbers	1,240	39.2%
• Extended	49	1.6%

RP Study - Character Sets

Number & percentage of passwords with only:

Lowercase + uppercase	1186	37.5%
Lowercase + numbers	593	18.7%
Lowercase	592	18.7%
Lowercase + upper + numbers	327	10.3%
Numbers	211	6.7%
Uppercase	112	3.5%
Uppercase + numbers	93	2.9%
Lowercase + extended	23	0.7%
Lowercase + upper + extended	10	0.3%
Lowercase + upper + num + ext	8	0.3%
Lowercase + number + extended	6	0.2%
Numbers + extended	1	0.03%
Uppercase + number + extended	1	0.03%

RP Study - Character Sets

Total characters in passwords:

Lowercase	13,967	68.3%
Numbers	3,536	17.3%
Uppercase	2,887	14.1%
Extended	57	0.3%

20,447 characters total

RP Study - Character Summary

Most passwords in this study contained large amounts of lowercase letters

Almost 50% of the passwords consisted of only lowercase, uppercase or lower+uppercase characters.

RP Study - Lengths

The length of a password is one of the easiest factors to change when you want to increase the strength of your passwords.

Unfortunately, you usually run into problems with particular OS restrictions and the ability of a user to recall longer strings.

$95^{(1\ldots8)} - 95^{(1\ldots6)} = 6{,}704{,}038{,}042{,}500{,}000$

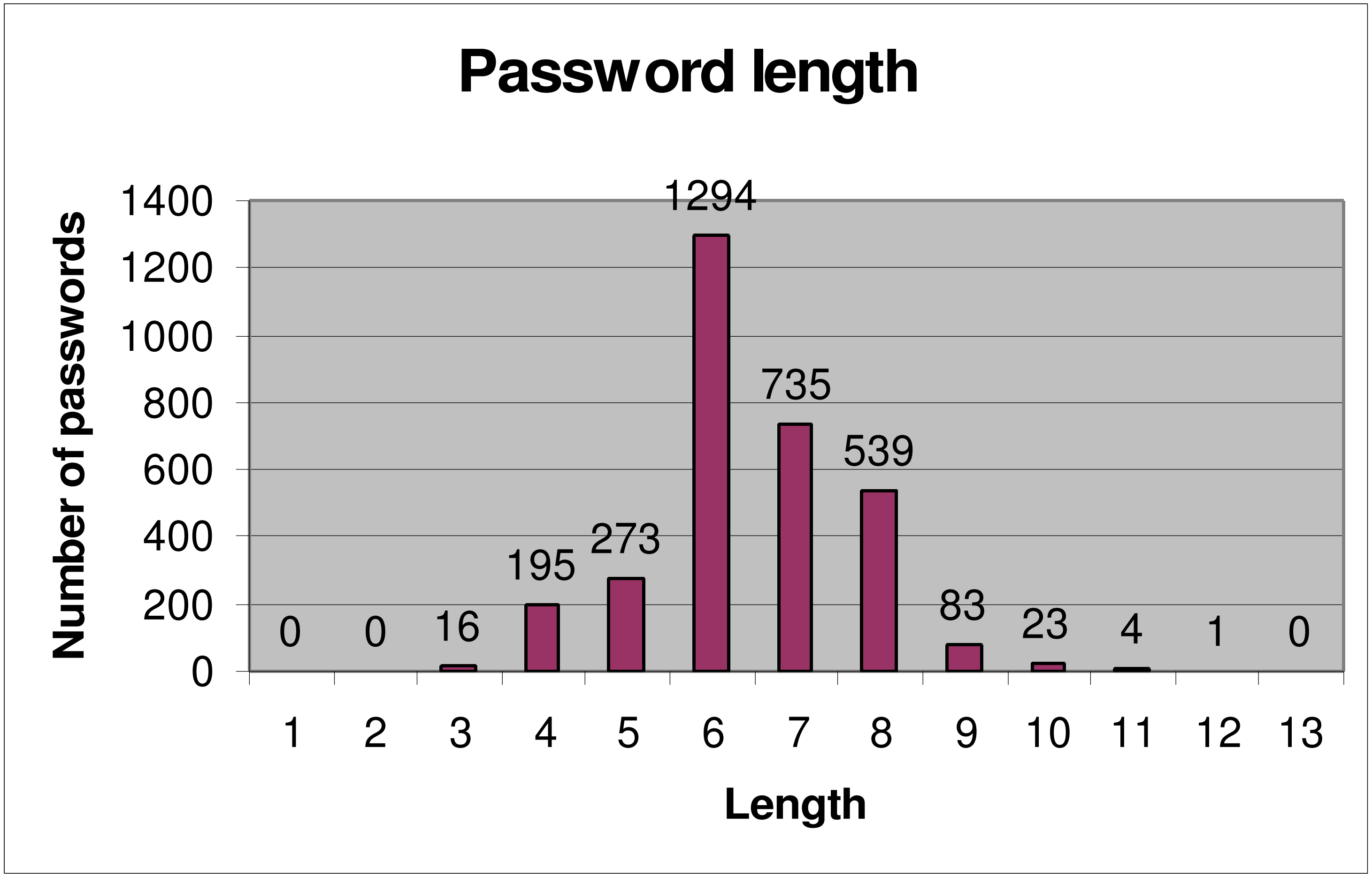
RP Study - Length

Password lengths:

Passwords with 3 characters:	**16**	**0.51%**
Passwords with 4 characters:	**195**	**6.2%**
Passwords with 5 characters:	**273**	**8.6%**
Passwords with 6 characters:	**1294**	**40.9%**
Passwords with 7 characters:	**735**	**23.2%**
Passwords with 8 characters:	**539**	**17.0%**
Passwords with 9 characters:	**83**	**2.6%**
Passwords with 10 characters:	**23**	**0.73%**
Passwords with 11 characters:	**4**	**0.13%**
Passwords with 12 characters:	**1**	**0.03%**

Average length is 6.5 characters

RP Study - Length



RP Study - Data comparison

Robert Morris, Sr. & Ken Thompson,
Password Security: A Case History

- Analyzed 3,289 cleartext passwords in 1980’s

“On a PDP-11/70, the time required to search through all character strings of length 8 from a 36 character alphabet is 112 years.”

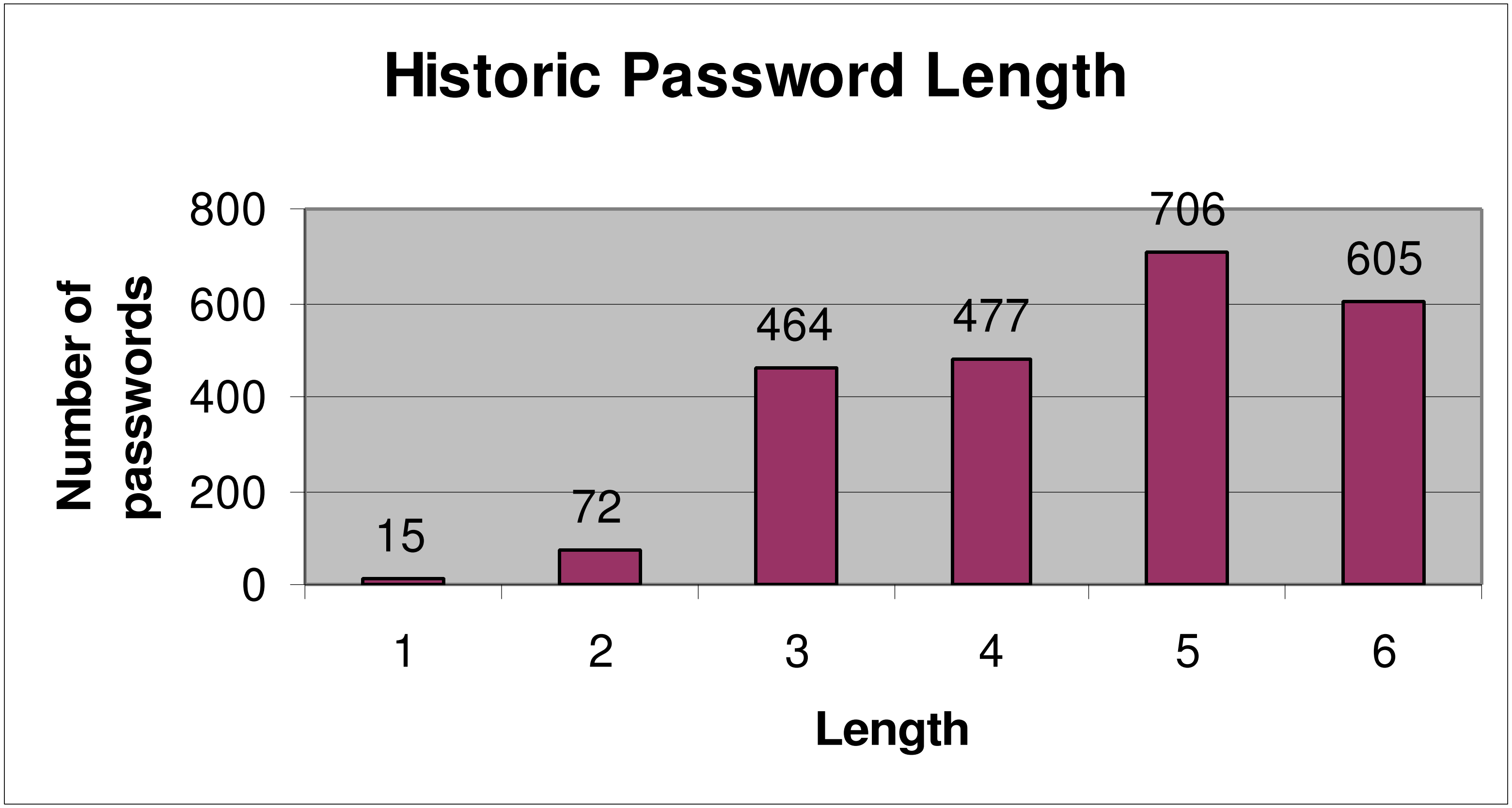
RP Study - Length comparison

Password lengths:

1 character	**15**	**0.5%**
2 characters	**72**	**2.2%**
3 characters	**464**	**14.1%**
4 characters	**477**	**14.5%**
5 characters	**706**	**21.5%**
6 characters	**605**	**18.4%**

Average length is: 4.5 characters

RP Study - Length comparison



For some reason this only accounts for 2,339 passwords

RP Study - Length summary

54% of the passwords fell between 3 and 6 characters in length.

In approximately 20 years, the average length of a password has only increased by 2 characters while computing power has skyrocketed.

RP Study - Password Duplication

We found that 158 passwords (or 5%) were also chosen by another user on the system.

- 1 password with 8 occurrences
- 2 passwords with 6 occurrences
- 2 passwords with 5 occurrences
- 9 passwords with 4 occurrences
- 32 passwords with 3 occurrences
- 112 passwords with 2 occurrences

RP Study - Password Duplication

It was interesting to find that in this study, hacker folklore (or at least the movie “Hackers”) isn’t right about the four most common passwords.

These are typically believed to be “love”, “sex”, “secret” and “god”.

Unfortunately, “password” rose into the number 4 position with 5 occurrences, while “secret” did register with 2 uses.

RP Study - Password Duplication

This means that for every 20 passwords you find, there is a good chance that one of the passwords will also be chosen by another user. This can also be true for independent systems.

These duplicated passwords also tend to fall into already easily guessable categories like dictionary words or names.

RP Study - Results by Category

Passwords were placed into 21 various categories based on their perceived group characteristics.

They are presented in order from what we believe are the easiest to guess to the hardest to guess.

RP Study - Password = Username

This category probably makes up the worst possible choice of passwords, because of the ease in guessing it.

There were 31--or 1% of the total--passwords that were also the username of the individual. 2 of these were the username backwards, with the remaining 29 being straightforward.

RP Study - Password = Username

The capitalization of the password was about the only factor which wasn’t immediately obvious:

- 11 No change (lowercase)
- 8 First letter capitalized
- 6 All caps
- 2 First & Last capitalized
- 1 All vowels capitalized
- 1 All consonants capitalized
- 2 Misc. capitalized

RP Study - Dictionary Words

As the second worst category to choose from, the use of dictionary words were definitely too widespread.

Using 10 word lists we were able to effectively find 999 passwords or 31.6% of the total.

RP Study - Dictionary Words

Word lists came from:

ftp://ftp.cdrom.com/pub/security/coast/dict

Used:

Unabr.dict.gz
algae.gz
myths-legends.gz
bacteria.gz
wordlist.zip
asteroids.gz
tolkien_words.gz
compass.zip
jargon.z
dictwl.tar

RP Study - Dictionary Words

Word lengths:

• 3 characters:	12	1.2%
• 4 characters:	79	7.9%
• 5 characters:	150	15.0%
• 6 characters:	408	40.8%
• 7 characters:	211	21.1%
• 8 characters:	120	12.0%
• 9 characters:	18	1.8%
• 10 characters:	1	0.1%

Average length is 6.2 characters

RP Study - Dictionary Words

Capitalization of the passwords:

312	Lowercase
40	Uppercase
539	First letter capitalized
13	Last letter capitalized
18	First & Last capitalized
17	All vowels capitalized
4	All consonants capitalized
56	Misc. capitalized

RP Study - Dictionary Words Comparison

Robert Morris Sr. & Ken Thompson, Password Security: A Case History

Their study found that 492 passwords -- or 15% of the total -- appeared in dictionaries and name lists.

Based on that data, it appears that the problem of bad password choices is getting worse.

RP Study - Names

This category easily contests for the second worst choice in passwords besides dictionary words.

Had we taken the time to research each user’s background, it might have been much easier to determine which names they would use.

159 (5%) passwords were found using 4 name lists.

RP Study - Names

Name lists came from:

ftp://ftp.cdrom.com/pub/security/coast/dict

Used:

male-names.gz
female-names.gz
family-names.gz
given-names.gz

RP Study - Names

Name Lengths:

4 characters:	7	4.4%
5 characters:	30	18.9%
6 characters:	66	41.5%
7 characters:	40	25.2%
8 characters:	14	8.8%
9 characters:	2	1.3%

Average length is 6.2 characters

RP Study - Names

Capitalization of the passwords:

49	Lowercase
9	Uppercase
87	Capital only as the first character
2	Capital only as the last character
5	Capital as the first and last characters
0	All vowels capitalized
1	All consonants capitalized
6	Capitals as middle characters

RP Study - Numbers

At first glance, choosing a number for a password may not seem like a bad idea. However, due to the limited character set and the common trend in using a number that can be easily guessed, numeric passwords aren’t wise.

211 numeric passwords making up 6.7%

RP Study - Numbers

Number Lengths:

3 characters:	2	1.0%
4 characters:	64	30.3%
5 characters:	11	5.2%
6 characters:	107	50.7%
7 characters:	7	3.3%
8 characters:	15	7.1%
9 characters:	4	1.9%
10 characters:	1	0.5%

Average length is 5.6 characters

RP Study - Numbers

- 60 passwords fit the format for a valid birth date.
- 16 passwords fit the format for a valid year before 2000
- 5 passwords were sequential (1234..)
- 1 password was a possible local zip code
- Other passwords fit formats for phone numbers, SS#s, radio stations, addresses,etc.

RP Study - Word or Name +

Adding a number to a word or name is often though of as a good way to increase security. Unfortunately, that doesn’t seem to hold true.

459 passwords (14.5%) found that were a word or name plus a number.

RP Study - Word or Name +

Word/Name + # Lengths:

4 characters:	7	1.5%
5 characters:	20	4.4%
6 characters:	201	43.8%
7 characters:	137	29.8%
8 characters:	81	17.7%
9 characters:	10	2.2%
10 characters:	3	0.7%

Average length is 6.7 characters

RP Study - Word or Name +

Number format & placement:

- Number at the beginning of the word: 53
- Number at the end of the word: 406
- 208 1 number
- 137 2 numbers
- 49 3 numbers
- 60 4 numbers
- 4 5 numbers
- 1 6 numbers

RP Study - Word or Name +

Number format & placement:

- **There were 81 uses of the number: 0**
- **There were 256 uses of the number: 1**
- **There were 113 uses of the number: 2**
- **There were 74 uses of the number: 3**
- **There were 67 uses of the number: 4**
- **There were 61 uses of the number: 5**
- **There were 57 uses of the number: 6**
- **There were 66 uses of the number: 7**
- **There were 47 uses of the number: 8**
- **There were 73 uses of the number: 9**

RP Study - Word or Name +

Capitalization of the passwords:

254	Lowercase
20	Uppercase
152	Capital only as the first character
6	All vowels capitalized
3	All consonants capitalized
24	Capitals as middle characters

RP Study - Word + Word

While putting two words together in a password is better than one word alone, it won’t stop a determined attacker.

362 passwords (11.5%) found.

RP Study - Word + Word

Word + Word Lengths:

• 4 characters:	1	0.3%
• 5 characters:	7	1.9%
• 6 characters:	120	33.1%
• 7 characters:	106	29.3%
• 8 characters:	101	27.9%
• 9 characters:	23	6.4%
• 10 characters:	4	1.1%

Average length is 7.1 characters

RP Study - Word + Word

Capitalization of the passwords:

- 114 Lowercase
- 24 Uppercase
- 147 Capital only as the first character
- 6 Capital only as the last character
- 7 Capital as the first and last characters
- 6 All vowels capitalized
- 1 All consonants capitalized
- 57 Capitals as middle characters

RP Study - Name + Character

Adding a character to a name typically adds some time to hacking efforts, but often that additional character is the initial of the user’s first or last name.

Found 65 for 2.1%

RP Study - Name + Character

Name + Character Lengths:

• 4 characters:	6	9.2%
• 5 characters:	9	13.9%
• 6 characters:	40	61.5%
• 7 characters:	8	12.3%
• 8 characters:	1	1.5%
• 9 characters:	1	1.5%

Average length is 5.9 characters

RP Study - Name + Character

Capitalization of the passwords:

31	Lowercase
0	Uppercase
22	Capital only as the first character
4	Capital only as the last character
3	Capital as the first and last characters
0	All vowels capitalized
1	All consonants capitalized
4	Capitals as middle characters

RP Study - Word + Character

Adding an extra character to a word often just makes it plural, descriptive or just happens to find another similar word.

75 found for 2.4%

RP Study - Word + Character

Word + Character Lengths:

• 4 characters:	8	10.7%
• 5 characters:	13	17.3%
• 6 characters:	35	46.7%
• 7 characters:	8	10.7%
• 8 characters:	11	14.7%

Average length is 6.0 characters

RP Study - Word + Character

Capitalization of the passwords:

- 20 Lowercase
- 8 Uppercase
- 30 Capital only as the first character
- 2 Capital only as the last character
- 5 Capital as the first and last characters
- 2 All vowels capitalized
- 0 All consonants capitalized
- 8 Capitals as middle characters

RP Study - Username variation

Some users think they're being smart to choose a variation of their username instead of using an exact match.

71 found for 2.2%

RP Study - Username variation

Patterns:

- Using initials followed by a number (date)
- Adding a number or character
- Removing a character
- Using one of the username components
- Repeating the username

RP Study - Username variation

Capitalization of the passwords:

38	Lowercase
6	Uppercase
19	Capital only as the first character
1	Capital only as the last character
0	Capital as the first and last characters
0	All vowels capitalized
1	All consonants capitalized
6	Capitals as middle characters

RP Study - # for Character Subs.

What we would term “3l1t3” speak is used in passwords to make them harder to guess.

9 for 0.3%

Examples “1” for “I”,“VV” for “w”, “3” for “E”

RP Study - Repeating / Patterns

Patterns of numbers, characters or words within passwords aren't too uncommon either.

Repeating pattern or word: 18 (0.6%)

Repeating pattern with character in the middle: 5 (0.2%)

Ave. Length: 6.3 characters

RP Study - Word variations

Word with an extra character in the middle:

11 (0.3%) AveLen: 6.8

Word + Word + char or word + char + word or char + word + word:

85 (2.7%) AveLen: 7.3

Special word (word + characters or numbers):

36 (1.1%) AveLen: 6.6

Numbers + Word + Numbers:

14 (0.4%) AveLen: 6.9

RP Study - Phrases

Phrases (3 or more words/abbreviations):
53 (1.7%)

Common usage / terms:
“Iluvyou”, “goforit”, “iamgod”, “1ofmany”

Average Length: 7.7

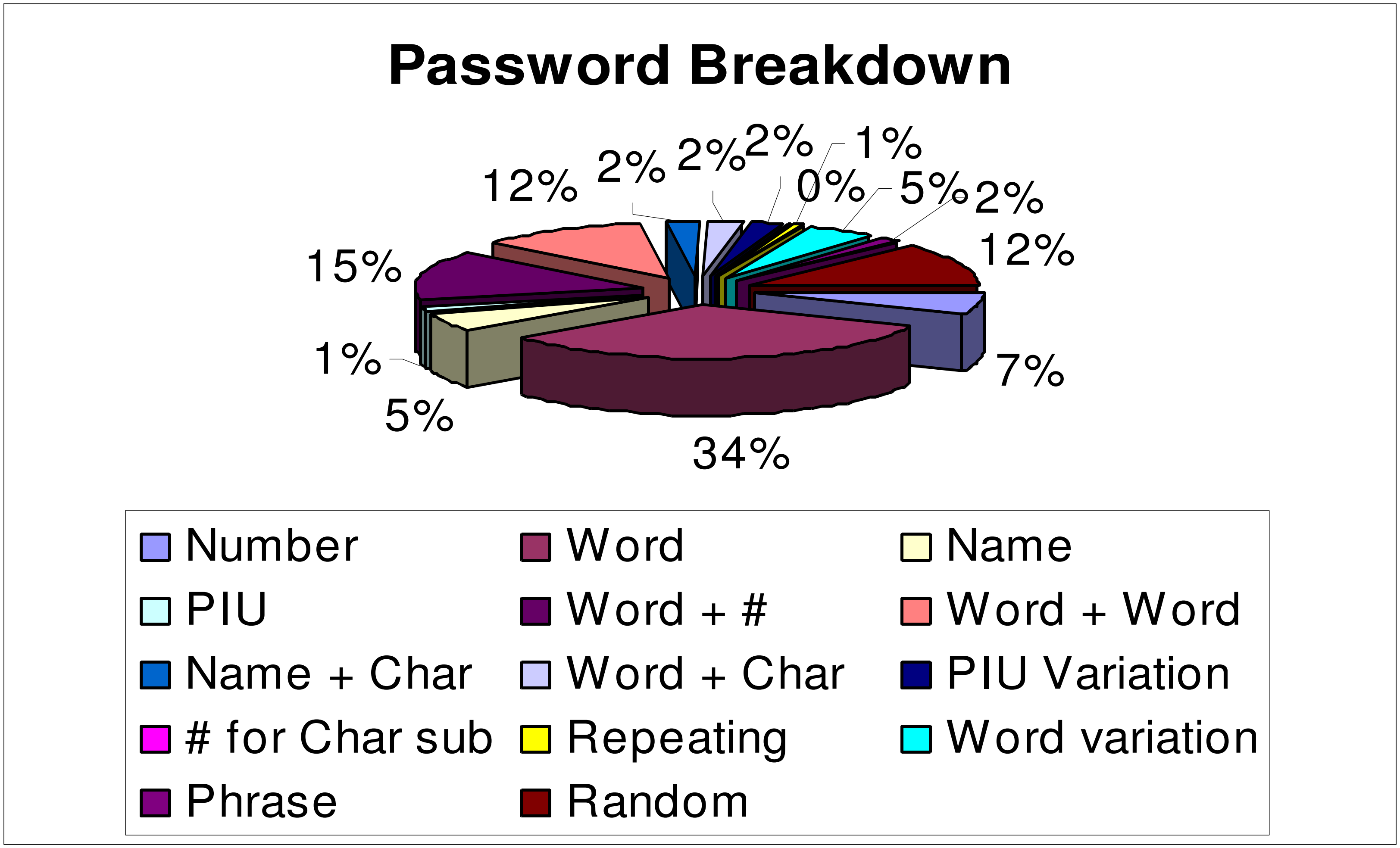
RP Study - Random?

Limited random (1 character set):
62 (2.0%) AveLen: 6.3

Semi-random (2 character sets):
243 (7.7%) AveLen: 6.8

Random (3+ character sets):
72 (2.3%) AveLen: 7.1

RP Study - Summary of Data



RP Study - Summary of Data

Most effective word lists:

- Unabridged dictionary: 410
- Dictwl: 211
- Female-name: 83
- Family-names: 57
- Given-Names: 15
- Bacteria: 4
- Myths & Legends: 1

Word list: 1688

Male-name: 167

Common passwords: 61

Jargon: 24

Asteroids: 6

Tolkien: 2

Algae: 1

RP Study - Summary of Data

Predictions on Future Password Trends

- Password length won’t substantially increase without OS requirements.
- Without guidance or enforcement, passwords will become easier to guess.
- People will be using the same password on various independent systems.
- Poor passwords will continue to be the leading breech of system security.

Alternatives to Reusable Passwords - What You Have

“What you have” - Physical access devices

Advantages:

- Loss of the object should alert user to possible attack (unlike the loss of a password).
- Typically difficult to spoof without possession of the object.
- The object can be reclaimed & reused upon the user’s absence or termination.

Alternatives to Reusable Passwords - What You Have

Disadvantages

- Must be complex enough to discourage & impede duplication.
- Higher cost & learning curve than password systems.
- Object is only loosely associated with the authorized user.
- User may not physically secure the object.

Alternatives to Reusable Passwords - What You Have

Magnetic cards:

- Cheap.
- Fairly easy to implement.
- Can be used for multiple purposes.
- Also easy to duplicate.

Alternatives to Reusable Passwords - What You Have

One-time-password generators:

- Come in both hardware and software form
- www.securitydynamics.com
- www.activecard.com

Alternatives to Reusable Passwords - What You Have

Smart Cards:

- Allow you to store public and private keys
- www.litronic.com
- www.datakey.com
- www.datacard.com

Alternatives to Reusable Passwords - What You Are

Biometrics has been receiving a lot of media attention in the last year or so. This is a good sign that the technology is becoming more mature and accepted.

"Of the projected $100 million [total expenditures to create biometric security systems], governments will spend approximately $62 million and corporations $38 million."

-- Howard Millman, InfoWorld 6/29/98

Alternatives to Reusable Passwords - What You Are

The Biometric Consortium

http://www.biometrics.org/

- Disneyland (season tickets)- Hand geometry
- MasterCard (access)- Fingerprints
- Mr. Payroll (check cashing) - Face recog.
- BT (calling card)- Iris scanning
- INS (border)- Hand geometry

Alternatives to Reusable Passwords - What You Are

Types of biometrics:

- Fingerprint - Estimated to account for 80% of devices
- Retina
- Iris
- Blood vessels in arm
- Hand/finger geometry
- Facial recognition
- Keyboard dynamics
- Signature analysis
- Voice recognition

Alternatives to Reusable Passwords - What You Are

Advantages

- Authentication feature is directly associated with the proper user.
- Complexity of features make it harder to duplicate (www.networkcomputing.com).
- User isn’t burdened with physical devices or memorizing phrases.

Alternatives to Reusable Passwords - What You Are

Disadvantages

- Readers/Analyzers must be properly tuned to permit some tolerance.
- Additional costs for scanning/analyzing equipment.
- May cause privacy concerns.
- Might not be compatible with all systems.

Alternatives to Reusable Passwords

Future developments in authentication

- Combination devices
- Don’t invade privacy
- Standard format between vendors
- Don’t create the ‘Ident-A-Ease’!

Suggestions & Solutions

Okay, passwords are bad but what can I do to secure our systems?

"Any effort to improve passwords must be concerned with the trade-off between user memory and security."

--Abadi, Lomas & Needham - Strengthening Passwords

Suggestions & Solutions

At the very least, strengthen your existing password systems

- Improve length requirements
- Check against username and other likely choices
- Enforce regular, but not overly-frequent changes
- Run your own attacks against the system to see if it can withstand them
- Educate users as to their role in system security

Suggestions & Solutions

Password system improvements (cont.):

- Audit password changes and invalid logins.
- Establish a timely review of your audit logs.
- Lock out accounts after X invalid attempts.
- Don’t allow easy access to your password file.
- Limit the methods of usurping authentication by privileged users.

Conclusion

Technology is outpacing our ability to easily protect ourselves from outside security attacks.

Make sure you're not indifferent to the threat and take action today!

Share this knowledge and help cause a paradigm shift in authentication.

Conclusion

Stay vigilant

Remember when systems lock down security in one area, hackers increase their attacks on other points in the system.

Conclusion

Thanks for your time & patience!

Please direct any questions, comments or grievances to:

bkmarsh@feist.com

316-393-7233