

Passwords

David Morgan

© David Morgan 2006

What's makes bad ones?

- only words or numbers (09112002, hackme)
- recognizable words (john1, R2D2)
- foreign language words (bonjour1, hastalavistababy)
- hacker terminology (H4XOR, 1337)
- personal info (names, birthdates, addresses)
- reverse words (nauj, esrever)

© David Morgan 2006

What's makes good ones?

- at least 8 characters
- mixed case
- mixed letters and numerals
- punctuation/non-alphanumeric symbols included
- something you can remember

© David Morgan 2006

Making a good one

- think of a memorable phrase (wasn't that a dainty dish to set before the king)
- make it an acronym (wtaddtsbtk)
- substitute non-letters for letters (w7@dd7sb7k)
- capitalize something (w7@DD7sb7k)

© David Morgan 2006

Forcing strong passwords

- create them for users, don't let users change them
- use PAM's pam_cracklib module
- add other PAM modules
 - pam_passwdqc (<http://www.openwall.com/>)

© David Morgan 2006

Password crackers

- John the Ripper (<http://www.openwall.com/>)
- Crack (<http://www.crypticide.com/dropsafe/info/home.html>)
- Slurpie (<http://www.ussrback.com/distributed.htm>)

© David Morgan 2006

Is guesswork easy or hard?

- An alphabet is a set of symbols
- How many words of a certain length can you compose from an alphabet?
- Depends on
 - the number of symbols in the alphabet
 - the particular wordlength

© David Morgan 2006

Is guesswork easy or hard?

- | | |
|---------------------------|----------------------------|
| ● a 2-symbol alphabet has | ● a 10-symbol alphabet has |
| – 2 one-letter words | – 10 one-letter words |
| – 4 two-letter words | – 100 two-letter words |
| – 8 three-letter words | – 1000 three-letter words |
| ● a 3-symbol alphabet has | ● an n-symbol alphabet has |
| – 3 one-letter words | – n one-letter words |
| – 9 two-letter words | – n^2 two-letter words |
| – 27 three-letter words | – n^3 three-letter words |

© David Morgan 2006

How many words are there?

- 26-letter alphabet, wordlength 3: 17576
- 26-letter alphabet, wordlength 6: 308,915,776
- 52-letter alphabet, wordlength 3: 140,608
- 52-letter alphabet, wordlength 6: 19,770,609,660

- a fish is in a pond – harder to catch in a bigger pond

© David Morgan 2006