

## Re: Password Cracking

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-01/0516.html>

---

**From:** Lohkee ([Lohkee@worldnet.att.net](mailto:Lohkee@worldnet.att.net))

**Date:** 01/24/03

From: "Lohkee" <[Lohkee@worldnet.att.net](mailto:Lohkee@worldnet.att.net)>

Date: Fri, 24 Jan 2003 01:08:17 GMT

"Ernst-Udo Wallenborn" <[ernst-udo.wallenborn@freenet.de](mailto:ernst-udo.wallenborn@freenet.de)> wrote in message news:s51znpr3pt.fsf@dilbert.pointyhairedbosses.de...

>

> "Lohkee" <[Lohkee@worldnet.att.net](mailto:Lohkee@worldnet.att.net)> writes:

>

>> *You statement is absolutelty FALSE. I have stated, and maintain, that*

>> *password strength is a function of the number of possibilities in the pool.*

>> *The greater the number, the "stronger" a given password – a FACT which is*

>> *easily proven by mathamatical analysis, although I must admit, I do wish*

>> *lottery people would use your method.*

>

>

> *This is simply not true.*

>

>

>

> --

> Ernst-Udo Wallenborn

Why? Because you say so? Contrast your "proof" ("this is simply not true") with mine: Given a known number of possibilities, we can calculate the odds of the attacker being able to guess the correct sequence (password) on the first attempt. Many papers have been written on the subject of password length, and they all – that I know of – conclude that a longer password is stronger. Why? Because the odds against guessing the correct one grow as the numbers of possibilities are increased. We can prove this mathematically. No one seems to have too much difficulty with this concept. Yet, for some completely bizarre reason, they gag on the reverse, i.e., that the odds in favor of the attacker increase as the number of possibilities to choose from is decreased (which is completely irrational to say the least). We can also prove this mathematically. Security through science or security through superstition. We all have a choice.

Lohkee!