A Study of various combinations of password rule parameters vs. LOA[[1]](#footnote-1) (#) criteria.

# Overview:

Authentication is a common, first level of system security. “Increase the likelihood that you are who you claim to be.” Lively discussions initiate over the exact rules that are “the most secure” for traditional passwords.

One may argue that the most secure settings are those that are documented and enforced, rather than the exact parameter settings. A balance of the needs of those using a system, with those supporting the systems and those accountable for the privacy and integrity of the system’s contents is best reached through productive discussions.

To aid in the productive discussions, and show the inter-play between password criteria settings, we have created a tool.

A dynamic spreadsheet was created, based on NIST publication 800-63, *Electronic Authentication Guidelines*. It presents three tables, all based on a system that accepts any character from a 94 characters set. Each table gains “security” through added rigor in the password model. Basically, each increase in requirements is a method of forcing higher degrees of entropy (randomness) in a self-chosen password.

Example 1 – Base line for this discussion

The passwords are forced to be changed every 180 days.

One can make an incorrect password guess 10 times before the credential is locked out from system access.

The lockout is for 100 hours. (Essentially forcing a call to the “help desk”.)

*Findings – passwords must be 9 characters long to reach LOA2 compliance, if no additional rules are enforced.*

Example 2 – Increase the life of a password

The passwords are forced to be changed every 360 days.

One can make an incorrect password guess 10 times before the credential is locked out from system access.

The lockout is for 100 hours. (Essentially forcing a call to the “help desk”.)

*Findings – doubling of the life of the password does not change the criteria required for LOA2 compliance.*

Example 3 – Same password life, but decreased lockout time

The passwords are forced to be changed every 182 days.

One can make an incorrect password guess only 3 times before the credential is locked out from system access.

The lockout is 15 minutes.

*Findings: - drastically decreasing the lockout time period has dramatic affects on password rules to meet LOA2 criteria. (1) LOA2 cannot be met without some complexity rules. (2) Even with complexity rules, the allowed erroneous guesses is reduced to only three AND passwords must be at least 10 characters long. So, increased # of lockouts should be anticipated.*

Example 4 – Extremely long password life

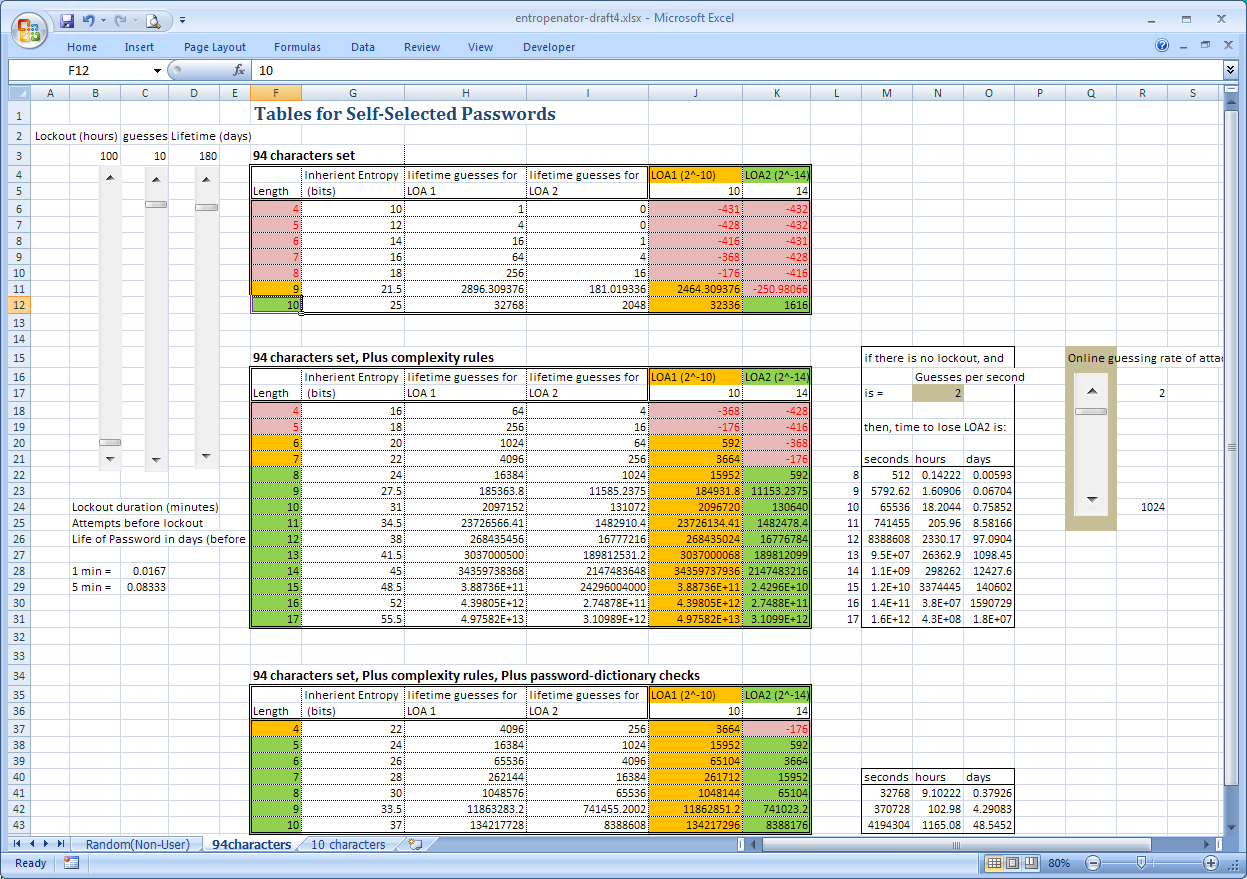
The passwords are forced to be changed every 10 YEARS (essentially never).

One can make an incorrect password guess 10 times before the credential is locked out from system access.

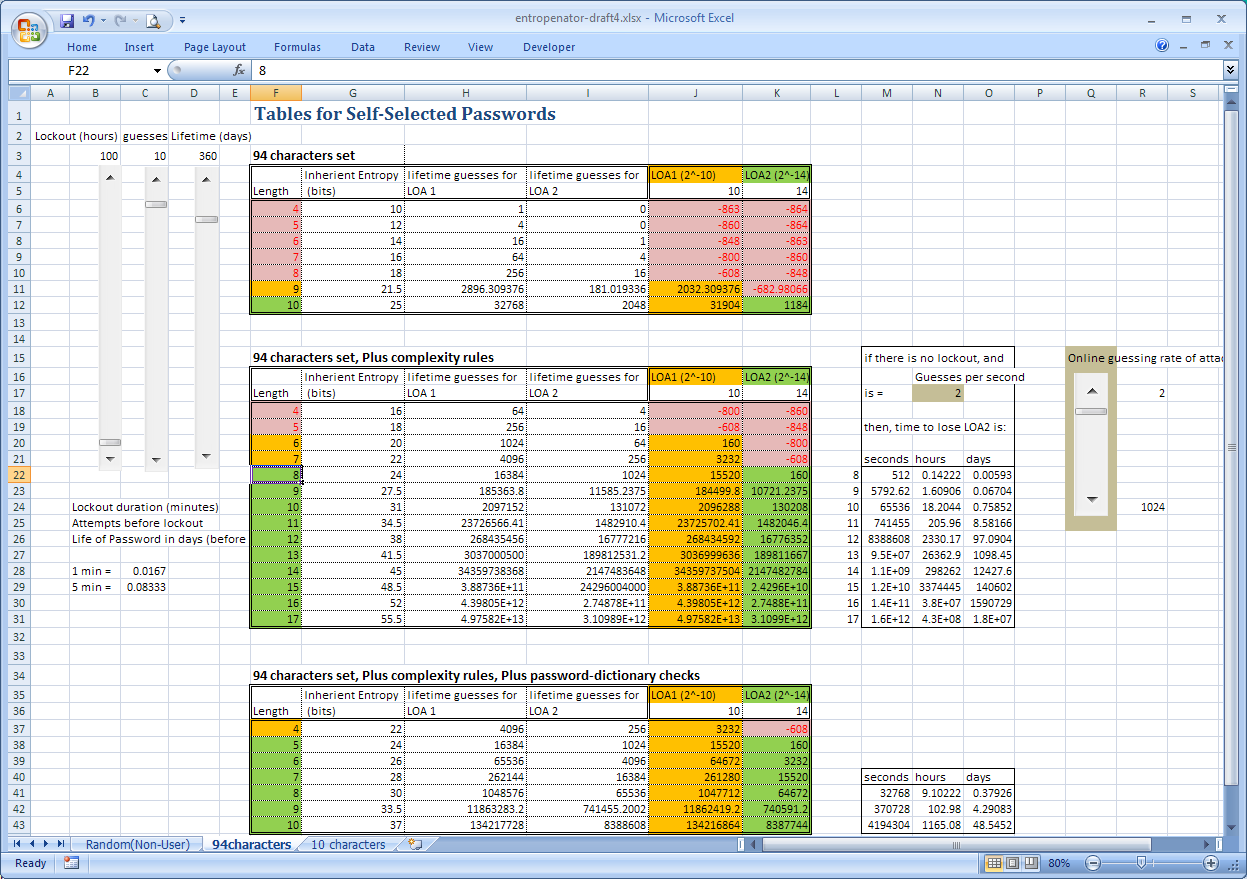
The lockout is 14 hours.

*Findings: - drastically increasing the password has dramatic affects on password rules to meet LOA2 criteria. (1) LOA2 cannot be met without some complexity rules. (2) Even with complexity rules, the lockout has to be at least 14 hours if we desire to allow 10 erroneous guesses, AND passwords must be at least 10 characters long. Lock outs would almost always generate a call for a reset.*

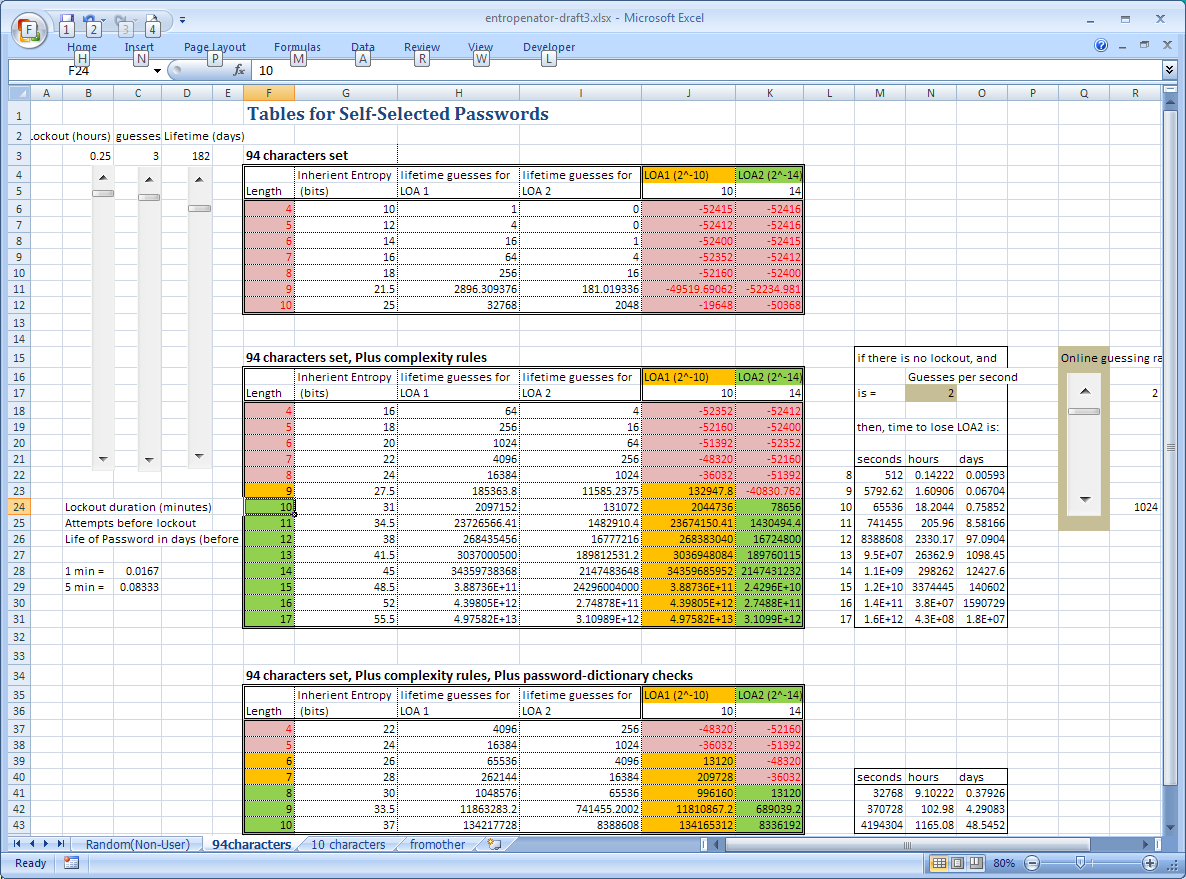
Example 1



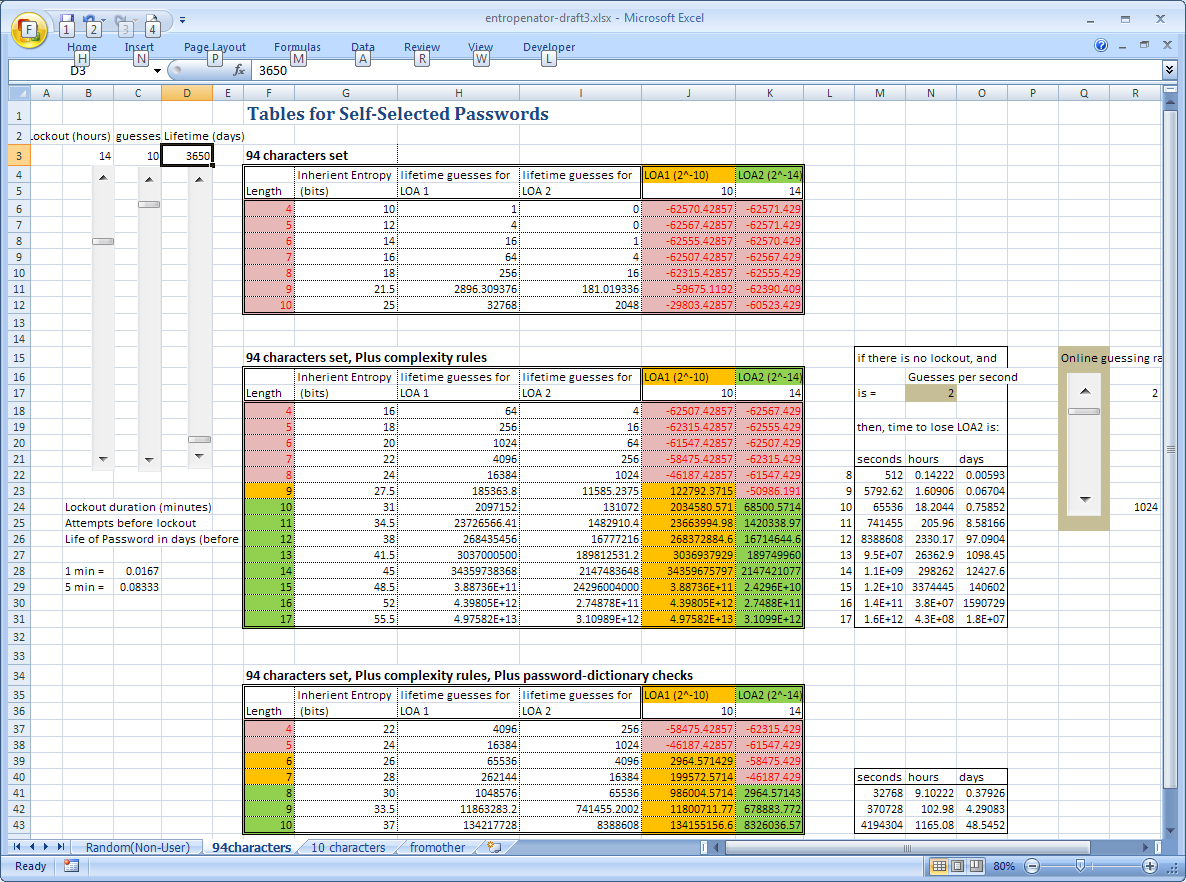
Example 2



Example 3



Example 4



1. LOA – Level of Assurance [↑](#footnote-ref-1)