

COB review by Dan Clapper

Title: “Perfect Passwords: Selection, Protection and Authentication”

Author: Mark Burnett

Length: 134 pages

Price: \$35.00

Reading time: 4 hours

Reading rating: 10 (1 = very difficult; 10 = very easy)

Overall rating: 4 stars (1 = average; 4 = outstanding)

If you’ve ever complained about password policies at your organization or felt that perhaps your passwords weren’t secure enough, Mark Burnett’s “Perfect Passwords” is the book for you.

According to the author the average adult in the US has to remember nine or more passwords, pin codes or other bits of secret information. These things can only do their job if they are difficult for a hacker to crack. Chapter 1 quickly shows why most people feel that they can choose good passwords, but in fact follow very predictable patterns that make them easy to crack.

Chapter 2 then follows up with a review of common techniques and software tools hackers use to exploit those weaknesses to guess your password. It turns out that most people choose very similar words when they have to create a password. Hackers have exploited this tendency by creating word “dictionaries” containing the most commonly used password words and various forms and using this dictionary along with software that uses this dictionary to try to login with each of these passwords. These dictionaries include many different versions of the words. For example, the author lists some of the possible passwords based on the word *dragon*: \$dragon, 108dragon, 4dragon4, dragon32, DRAGAN95, and so on. These password dictionary programs are freely available on the Internet and require no expertise to download and run.

Chapter 3 explores the foundations of password security. The author states that password security revolves around one key strategy: creating a password that no one can predict or guess. Randomness is one approach to making passwords that can’t be guessed. Unfortunately, it turns out that humans are very poorly equipped to either recognize or utilize randomness in choosing passwords. Since this chapter convincingly shows that using random character strings to decrease the predictability is not well suited to humans, the next chapter offers another approach to decreasing the predictability of passwords: choosing a wider variety of characters. Using this approach passwords should be a mix of lower case letters (what most people use) with upper case letters, numbers and characters such as *, #, -.

Building on this, Chapter 5 then details one of the author’s core principles for creating secure passwords: make them long! If a password is long enough, they will be hard to guess no matter how you build them. The minimum password length the author suggests

is fifteen characters and he relates an anecdote of amusing others around him while he typed in a sixty three character password.

The first reaction on hearing this could be “I’ll never be able to remember a password that long!” That would certainly be true if the passwords were just a string of random characters, but the remainder of the book gives many strategies for creating long passwords that are surprisingly easy to remember and type.

One example strategy the author suggests is create your password in the form of a fake email by following this process: Think of the name of anything, then think of a meaningful, funny or ironic phrase related to that name. Then put them together and add a dot-com or similar extension to it. Two examples developed with this strategy are: Dr.Seuss@greeneggs.com and rover22@Rover-hates-cats.net. Both of these passwords are well over the fifteen-character minimum, they use upper and lower case letters, non-letter characters and the second one uses numbers also.

Creating secure passwords is a must these days and this is the best book I’ve seen to show how to do that. I would recommend this book to IT and non-IT people alike. Give one to your system administrator and give your kids a copy. Passwords show no signs of going away, so let this book show you how to create strong, secure passwords that will keep your online resources protected.

Dan Clapper is an associate professor and chair of the Business Computer Information Systems and Economics Department in the College of Business at Western Carolina University. He teaches application development for both the desktop and Web environments. For previously reviewed books, visit our web site at www.wcu.edu/cob/.