Chapter 17
The Cost Perspective of Password Security

Leandros Maglaras
 https://orcid.org/0000-0001-5360-9782
De Montfort University, UK

Helge Janicke
Cyber Security Cooperative Research Centre, Edith Cowan University, Australia

Mohamed Amine Ferrag
 https://orcid.org/0000-0002-0632-3172
Guelma University, Algeria

ABSTRACT

This study technically analyses the maximum number of combinations for common passwords up to 12 characters long. A maximum storage size necessary for the creation of a data base that holds all possible passwords up to 12 characters is also presented along with a comparison against the publicized cost of storage from popular cloud storage providers and the national budget for intelligence and defense activities of a nation. Authors prove that it is technically possible that any password could be computed within seconds with nothing more than currently commercially available components. The study concludes that it is possible that nation states or even combined nation states working in collaboration could or already have bought private citizens' and businesses' passwords revealing that it may already be an age where the password may not be a legitimate defense for privacy anymore.

INTRODUCTION

As Critical National Infrastructures are becoming more vulnerable to cyber attacks, their protection becomes a significant issue for any organization as well as a nation Moreover the synergy between the Industrial Control Systems and the Internet of Things (IoT) has emerged bringing new security challenges (Maglaras et al., 2018) making the deployment of an overlapping strategy based on security tools,

people, and processes a necessity. Traditional security mechanisms are both appropriate and effective means to defend the boundaries of an organisation or a nation. Firewall architectures, email scanning, DPI, VPNs, HIDS, NIDS are all established ways by which an organisation can reduce the opportunities for the ingress of malicious software into their environments. As a complimentary measure, the practice of locking-down unused ports, USB devices, use of access controls through corporate directories and the enforcement of least-privilege access all reduce the insider threat. One of the basic but important security measures that any organization must have in place is a password policy (Gupta et al., 2018) along with other defense mechanisms (Jiang et al., 2018, Almomani et al., 2013).

Without delving into the historical or philosophical descriptions of what a password is and purely concentrating on the modern-day scientific definition of a password, in business and computing terms, according to the Cambridge dictionary under "*Password" in Business English*" it states "*a secret word or combination of letters and numbers that you use to prove who you are when you use a computer, website, etc.:*" (Cambridge Dictionary, 2019). Obviously, this is inaccurate as it excludes special characters that are now commonplace in most corporate password policies. To this end, in this chapter when a password is mentioned, its definition will be 'a group of characters chosen by a user from the available character sets of modern computing hardware and software for the purposes of authentication'. Innately there are many variables with passwords, as they themselves are extracted out of our complex languages in all their forms, even if not representative of a definable word.

There are many complex and interesting theories surrounding passwords and this has sparked much discussion and interesting content such as the journal "Password Security as a Game of Entropies" (Rass et al, 2018) as well as initiating some truly inspiring mathematics. Also, we are witnessing an evolution in the art of the possible with emergence of Quantum Computing that is brings advancements in our understanding of physics. Quantum computing presents incredible opportunity for industry to potentially compute complex issues at an exponentially increased speed. However, it has been long since it was speculated that this dramatic increase in computing power could spell the death of the password and similar security defences that rely on complexity. This is well described in the paper "*Global catastrophic risk and security implications of quantum computers" (Major et al, 2015)*, and this view is supported by the authors. In this paper however, the authors are questioning the possible of the present, utilising only commercially of the shelf equipment available to everyone today.

Figure 1. Passwords rules
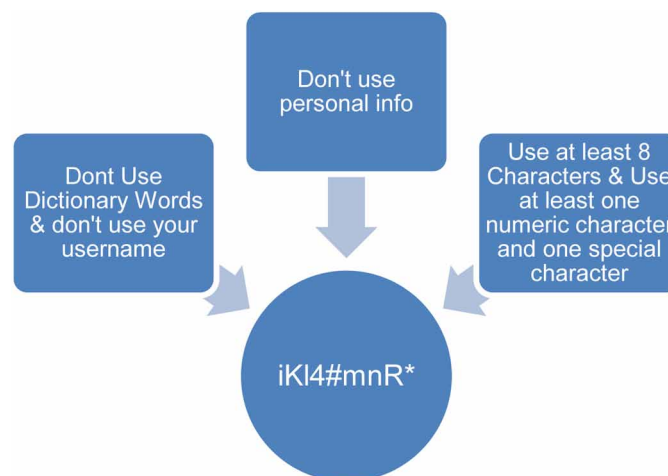
10 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/the-cost-perspective-of-password-security/253040

Related Content

The Use of Electronic Games in Distance Learning as a Tool for Teaching and Learning
Muhammet Demirbilek (2011). *Gaming and Simulations: Concepts, Methodologies, Tools and Applications (pp. 1233-1250).*
www.irma-international.org/chapter/use-electronic-games-distance-learning/49446

Construction and Application of Sentiment Lexicons in Finance
Kazuhiro Sekiand Masahiko Shibamoto (2018). *International Journal of Multimedia Data Engineering and Management (pp. 22-35).*
www.irma-international.org/article/construction-and-application-of-sentiment-lexicons-in-finance/196247

Analysis of Platforms for E-Learning
Maribel-Isabel Sánchez-Segura (2009). *Encyclopedia of Multimedia Technology and Networking, Second Edition (pp. 22-34).*
www.irma-international.org/chapter/analysis-platforms-learning/17378

Enhancing Rating Prediction by Discovering and Incorporating Hidden User Associations and Behaviors
Ligaj Pradhan (2019). *International Journal of Multimedia Data Engineering and Management (pp. 40-59).*
www.irma-international.org/article/enhancing-rating-prediction-by-discovering-and-incorporating-hidden-user-associations-and-behaviors/232181

On the Implementation of a Fragile Medical Image Watermarking Technique Using Saliency and Phase Congruency
Abhishek Basuand Soumadeb Dutta (2019). *Intelligent Innovations in Multimedia Data Engineering and Management (pp. 52-87).*
www.irma-international.org/chapter/on-the-implementation-of-a-fragile-medical-image-watermarking-technique-using-saliency-and-phase-congruency/211692